

**BEST AVAILABLE COPY****RESULT LIST**

2 results found in the Worldwide database for:

**jp2000285024** (priority or application number or publication number)

(Results are sorted by date of upload in database)

**1 PRINTER, PRINTING SYSTEM, PRINTING METHOD, AND RECORDING  
MEDIUM WITH PRINTING PROGRAM RECORDED THEREIN**

Inventor: FUJII MASAHIITO

Applicant: MINOLTA CO LTD

EC:

IPC: **B41J21/00; G06F3/12; H04N1/387** (+6)

Publication info: **JP2002086835** - 2002-03-26

**2 METHOD FOR ELECTRONICALLY STORING ORIGINAL GUARANTEE  
AND COMPUTER READABLE RECORDING MEDIUM RECORDING  
PROGRAM FOR EXECUTING THE METHOD BY COMPUTER**

Inventor: KANAI YOICHI; YANAIDA MASUYOSHI; (+2) Applicant: RICOH KK; NEW MEDIA DEV ASS

EC:

IPC: **G06F12/00; G06F12/14; G09C1/00** (+9)

Publication info: **JP2000285024** - 2000-10-13

---

Data supplied from the **esp@cenet** database - Worldwide

Patent number: JP2000285024

Publication date: 2000-10-13

Inventor: KANAI YOICHI; YANAIDA MASUYOSHI; SUGAO KIYOSHI; TOZAKI HIDEKAZU

Applicant: RICOH KK; NEW MEDIA DEV ASS

Classification:

- international: *G06F12/00; G06F12/14; G09C1/00; H04L9/32; G06F12/00; G06F12/14; G09C1/00; H04L9/32; (IPC1-7): G06F12/14; G06F12/00; G09C1/00; H04L9/32*

- european:

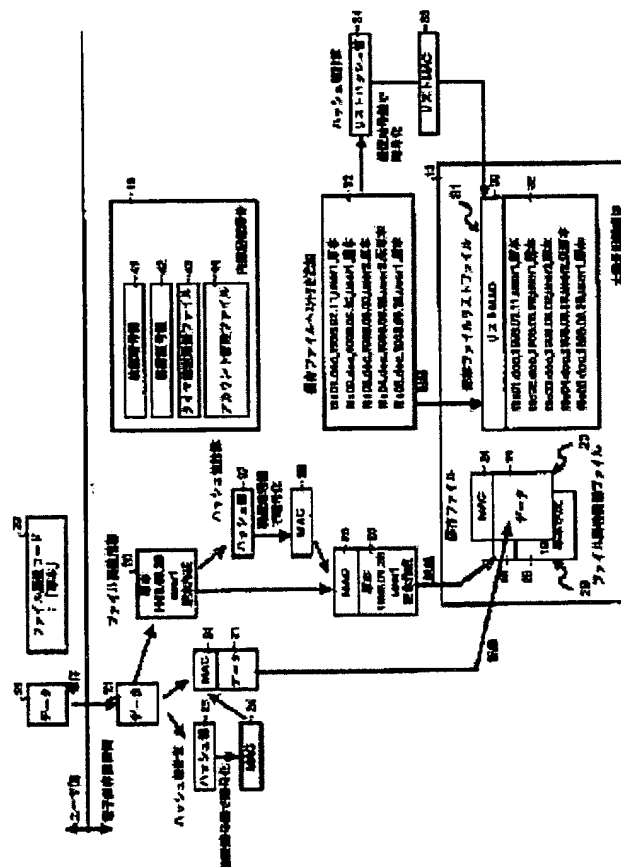
Application number: JP19990090212 19990330

Priority number(s): JP19990090212 19990330

## Abstract of JP2000285024

**PROBLEM TO BE SOLVED:** To improve the certification ability of electronic information by providing the electronic information with properties included in a paper original.

**SOLUTION:** In the case of storing electronic data 21, a file attribute code 22 indicating an original is added to the data 21 and the data 21 are stored in a state capable of discriminating it at least from other electronic data. The control level of an access to the original electronic data and the control level of an access to other electronic data can be respectively controlled.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-285024  
(P2000-285024A)

(43) 公開日 平成12年10月13日 (2000. 10. 13)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	チーゴト* (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 K 5 B 0 1 7
	5 3 7	12/00	5 3 7 A 5 B 0 8 2
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
	6 6 0		6 6 0 D 9 A 0 0 1
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 A
審査請求 未請求 請求項の数10 O L (全 26 頁)			

(21) 出願番号 特願平11-90212

(22) 出願日 平成11年3月30日 (1999. 3. 30)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(71) 出願人 596062738

財団法人ニューメディア開発協会

東京都港区三田1-4-28

(72) 発明者 金井 洋一

東京都大田区中馬込1丁目3番6号 株式  
会社リコー内

(74) 代理人 100089118

弁理士 酒井 宏明

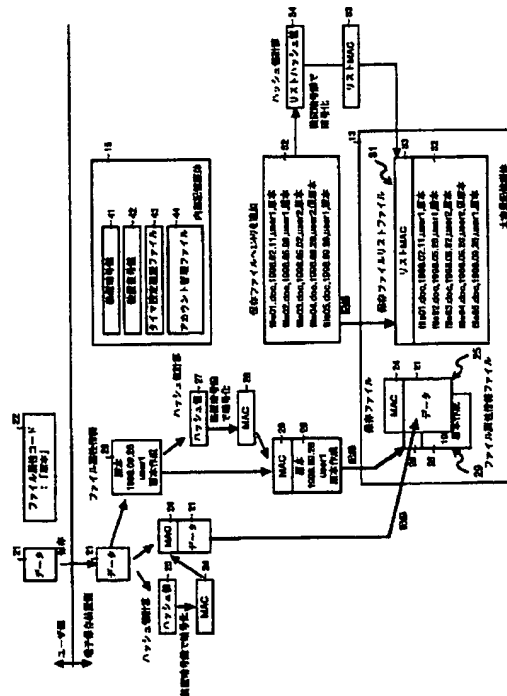
最終頁に続く

(54) 【発明の名称】 原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めること。

【解決手段】 電子データ21を保存する際に、原本であることを示すファイル属性コード22を付加し、少なくとも他の電子データとを識別可能な状態で保存するようにする。そして、原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御可能にする。



【特許請求の範囲】

【請求項1】 電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、前記原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御することを特徴とする原本性保証電子保存方法。

【請求項2】 前記電子データは、対応する属性情報と共に保存され、前記属性情報は、ユーザが編集入力を行えないように管理されており、前記原本の電子データに対し、前記属性情報として原本であることを示す属性コードを付与することを特徴とする請求項1に記載の原本性保証電子保存方法。

【請求項3】 さらに、前記原本の電子データに対する修正履歴を記録することを特徴とする請求項1または2に記載の原本性保証電子保存方法。

【請求項4】 さらに、前記原本の電子データに対する削除処理の実行を禁止することを特徴とする請求項1または2に記載の原本性保証電子保存方法。

【請求項5】 さらに、前記原本の電子データの複製を生成し、生成した複製を前記原本に対する謄本として管理することを特徴とする請求項1または2に記載の原本性保証電子保存方法。

【請求項6】 さらに、前記原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、前記原本の電子データと共に保存することを特徴とする請求項1または2に記載の原本性保証電子保存方法。

【請求項7】 さらに、前記電子データの移動が要求された場合に、前記電子データを対応する属性情報と共に移動させることを特徴とする請求項2に記載の原本性保証電子保存方法。

【請求項8】 さらに、前記原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、前記電子データがアクセスされた場合に、前記メッセージ認証子を用いて前記電子データに対する改ざんを検出することを特徴とする請求項2に記載の原本性保証電子保存方法。

【請求項9】 さらに、第1の保存装置に存在する前記電子データの複製を第2の保存装置に生成するための要求または前記第1の保存装置に存在する前記電子データを前記第2の保存装置に移動させるための要求があった場合に、第1の保存装置は、前記電子データおよび対応する属性情報のそれぞれに付与された前記メッセージ認証子を検証した後、前記メッセージ認証子を除いた電子データおよび対応する属性情報を前記第2の保存装置に転送し、前記第2の保存装置は、前記電子データおよび対応する属性情報を受け取り、処理内容に応じて前記属

性情報を変更し、前記電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存することを特徴とする請求項2に記載の原本性保証電子保存方法。

【請求項10】 前記請求項1～9のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、原本性保証電子保存方法に関し、より詳細には、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能な原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】情報の電子化の時代における情報管理の考え方として、セキュリティ (Security) とトラスティ (Trusty) というものがある。セキュリティとは、外部からのアタックにより電子情報が破壊されたり、盗まれてしまうことから防衛することである。一方、トラスティとは、電子情報が紙情報に比べて簡単に改ざんすることが可能である点に鑑み、電子情報の改ざんを防止することによって電子情報の証拠能力を確保することである。

【0003】上記トラスティには、第1の目的として、企業等の組織活動または個人活動が他より早く行われていたことを証明するという目的がある (優先権の主張)。ここで、第1の目的を達成するには、電子情報とその付随情報 (作成時期等) が改ざん不可能となっているか、または改ざんされても改ざんの事実を確実に検知できるようになっていることが必要である。現在、この目的に対する実用的な解としては、TTP (Trusted Third Party; 第三者認証機関) があり、その代表的なものとしては、米国の Surety 者が提供している認証サービスがある。

【0004】また、トラスティには、第2の目的として、企業等の組織活動または個人活動として不正が行われていないことを証明するという目的がある。ここで、第2の目的を達成するには、電子情報とその付随情報 (作成時期等) が改ざん不可能となっているか、または改ざんされても改ざんの事実を確実に検知できるようになっていることに加えて、電子情報ファイルが削除不可能または削除されたことが検知可能であることが必要である。この第2の目的は、環境や製造物責任等に対する企業の経営情報管理、官公庁等の情報公開等により今後ますます高くなってくると考えられている。この第2の目的を実現するためには、追記、修正等のバージョンアップや不正なファイル削除を防止するための機能が必要で、例えばローカルネットワークにおいて、ファイル管

理システムと一体化または連携した認証機能を有するシステムを用意することが好ましい。

【0005】

【発明が解決しようとする課題】ところで、現在は紙文書として保存することが法律で義務付けられている情報が多々存在しており、これが情報の電子化を阻害する要因となっているが、情報に原本性保証機能（真性性、保存性、見読性、原本の唯一性）を付与することにより、電子化が認められることになった（参照：総務庁通達等）。したがって、電子情報においても、紙ベースで構築されてきた法律体系に応じて原本と謄本とを区別できるようにすると共に、改ざんを容易に行えないようにし、電子情報の証明力を高めることが可能な技術の開発が望まれている。

【0006】また、原本性保証の対象となる情報は、前述した第2の目的に属する情報が大半であることから、ファイル管理システムと同じローカルエリアネットワーク上に存在する原本性保証サーバ、即ち、ユーザサイトに設置することが可能な原本性保証機能を有する認証サーバの実現が望まれている。これにより、例えば諸官庁の情報を扱うのに十分なトラスティとセキュリティを有した原本性保証サーバの実現が可能となる。

【0007】本発明は上記に鑑みてなされたものであって、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることを可能にすることを目的とする。

【0008】また、本発明は上記に鑑みてなされたものであって、ユーザサイトに設置可能な原本性保証機能を有する認証サーバを実現可能にすることを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するため、請求項1の原本性保証電子保存方法は、電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、前記原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御するものである。

【0010】また、請求項2の原本性保証電子保存方法は、請求項1に記載の原本性保証電子保存方法において、前記電子データが、対応する属性情報と共に保存され、前記属性情報が、ユーザが編集入力を行えないように管理されており、前記原本の電子データに対し、前記属性情報として原本であることを示す属性コードを付与するものである。

【0011】また、請求項3の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データに対する修正履歴を記録するものである。

【0012】また、請求項4の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法

において、さらに、前記原本の電子データに対する削除処理の実行を禁止するものである。

【0013】また、請求項5の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データの複製を生成し、生成した複製を前記原本に対する謄本として管理するものである。

【0014】また、請求項6の原本性保証電子保存方法は、請求項1または2に記載の原本性保証電子保存方法において、さらに、前記原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、前記原本の電子データと共に保存するものである。

【0015】また、請求項7の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、前記電子データの移動が要求された場合に、前記電子データを対応する属性情報と共に移動させるものである。

【0016】また、請求項8の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、前記原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、前記電子データがアクセスされた場合に、前記メッセージ認証子を用いて前記電子データに対する改ざんを検出するものである。

【0017】また、請求項9の原本性保証電子保存方法は、請求項2に記載の原本性保証電子保存方法において、さらに、第1の保存装置に存在する前記電子データの複製を第2の保存装置に生成するための要求または前記第1の保存装置に存在する前記電子データを前記第2の保存装置に移動させるための要求があった場合に、第1の保存装置が、前記電子データおよび対応する属性情報のそれぞれに付与された前記メッセージ認証子を検証した後、前記メッセージ認証子を除いた電子データおよび対応する属性情報を前記第2の保存装置に転送し、前記第2の保存装置が、前記電子データおよび対応する属性情報を受け取り、処理内容に応じて前記属性情報を変更し、前記電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存するものである。

【0018】さらに、請求項10のコンピュータ読み取り可能な記録媒体は、前記請求項1～9のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したものである。

【0019】

【発明の実施の形態】以下、本発明に係る原本性保証電子保存方法およびその方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体の一実施の形態について、添付の図面を参照しつつ詳細に説明する。

【0020】図1は、本実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。ユーザは、ホスト計算機2側からネットワーク（単なる通信路で良い）を介して電子保存装置1に対して電子データの保存処理や読み出し処理を実行することができる。

【0021】図1に示す電子保存装置1において、11はプロセッサを、12はネットワークを介して計算機2と通信を行うための通信ポートを、13は電子データを保存するハードディスクやCD-R等の大容量記憶媒体を、14は主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラム、復号プログラム等の原本性保証電子保存方法を実現するためのプログラムが格納されたEEPROM、ROM等で構成されたプログラム格納媒体を、15は装置暗号鍵、装置復号鍵、タイマ設定履歴ファイル、アカウント管理ファイル等が記憶されるEEPROM等で構成された内部記憶媒体を、16はアカウント名、ユーザ側内部認証鍵、ユーザ側外部認証鍵等が記憶されたICカード3が挿入されるICカードリーダー/ライタを、17はタイマをそれぞれ示している。

【0022】図1に示す大容量記憶媒体13としては、光磁気ディスクやCD-Rのように電子保存装置1から取り外し可能なものであっても良いが、その他のブロックは電子保存装置1として物理的に一体化されており、通信ポート12を介する以外に外部からアクセスできないように構成されている。すなわち、図1に示す電子保存装置1は、各ブロックに対して直接アクセスする方法のない耐タンパー性を持った装置である。

【0023】耐タンパー性を確保するレベルとしては、電子保存装置1の筐体を開けることができないようにシールを貼る程度のもので、筐体を開けられてしまった場合には装置が動作しなくなるようなものまで考えられるが、耐タンパー性を持たせることが可能であればどのようなものであっても良い。

【0024】図1に示す電子保存装置1は、ユーザから保存要求のあったデータを大容量記憶媒体13に記録するものである。その際、後にデータの改ざんを検出できるようにするため、保存するデータに対して電子保存装置1自身の暗号鍵によりメッセージ認証子を付加する。また、電子保存装置1は、大容量記憶媒体13に記録されているファイルのリストを作成し、それを大容量記憶媒体13に記録する処理を行う。このリストに対しても、同様にメッセージ認証子を付加する。

【0025】また、大容量記憶媒体13の不正なすり替えを検出するために、大容量記憶媒体13に記録されている保存ファイルリストと、それに付加されたメッセージ認証子を検出することで媒体の認証を行う。また、ファイルの作成日などに不正ができないよう、電子保存装置1に内蔵されているタイマ17から現在時刻を取得

し、ファイルの属性情報として管理する。

【0026】さらに、電子保存装置1内部で、オリジナルとコピーとを区別できるように、各ファイルには「仮原本」、「原本」、「謄本」といった属性を付与して管理する。属性の付与されていないファイルは「一般」ファイルと呼ぶことにする。「原本」の属性が付与されて管理されているファイルに対し、外部から複製の作成を要求すると、複製されたファイルには「謄本」という属性が付与される。この属性コードは、他のファイル属性情報と共に、データファイルと関連付けられたファイル属性情報ファイルとして大容量記憶媒体13に記録され、データファイルと同様、メッセージ認証子を付加して外部から変更することができないように管理される。大容量記憶媒体13を取り外して外部でその属性が改ざんされたような場合には、そのファイル属性情報ファイルに付与したメッセージ認証子を検証した際にその改ざんを検出することができる。

【0027】つぎに、前述した構成を有する電子保存装置1を用いて実行される原本性保証電子保存方法について、

- (1) ユーザ登録処理
- (2) 保存装置へのログイン処理
- (3) 電子データ保存処理
- (4) 大容量記憶媒体マウント処理
- (5) ファイル読み出し処理
- (6) 謄本作成処理
- (7) バックアップ作成処理
- (8) ファイル移動処理
- (9) ファイル削除処理
- (10) ファイル属性コード変更処理
- (11) ファイル追記処理
- (12) ファイル編集処理

の順で具体的に説明する。

【0028】(1) ユーザ登録処理

ここでは、ユーザが電子保存装置1を利用する際に、電子保存装置1とユーザとの間で相互認証を行う必要があるものとする。そのため、電子保存装置1に対して予めユーザ登録を行っておく必要がある。ここで、電子保存装置1には、予めシステム管理者用のICカードが付属しているものとする。クライアント（計算機2）に接続されたICカードリーダーにシステム管理者用のICカードを挿入してアカウント登録用のプログラムを起動し、ユーザ登録を行う。

【0029】図2は、ユーザ登録処理を示すフローチャートであり、図2(a)はクライアント側で実行されるユーザ登録処理を、図2(b)は電子保存装置1側で実行されるユーザ登録処理をそれぞれ示している。以下では、図2(a)および図2(b)の両方を用いてユーザ登録処理を説明する。

【0030】まず、図2(a)に示すように、システム

管理者用ICカードをクライアントのカードリーダーに挿入し(S11)、パスワードを入力する(S12)。そして、ICカードでパスワード照合が行われ(S13)、正しいパスワードでない、即ち不正なパスワードの場合(S14; No)、エラーとしてユーザ登録処理が終了となる。

【0031】一方、正しいパスワードの場合(S14; Yes)、図2(a)および図2(b)に示すように、電子保存装置1およびICカードとの間で相互認証処理が実行される(S15, S21)。そして、電子保存装置1およびICカードとの間で実行された相互認証処理が成功しなかった場合(S16, S22; No)、エラーとしてユーザ登録処理が終了となる。

【0032】また、電子保存装置1およびICカードとの間で実行された相互認証処理が成功した場合(S16, S22; Yes)、クライアントから電子保存装置1に対してユーザ登録が要求される(S17)。電子保存装置1は、クライアントからのユーザ登録の要求がシステム管理者からの要求か否かを判定し(S23)、システム管理者からの要求ではないと判定した場合(S23; No)、エラーとしてユーザ登録処理が終了となる。一方、システム管理者からの要求であると判定した場合(S23; Yes)、電子保存装置1は、ユーザ登録要求からアカウント名を取得する(S24)。ここで、新しいICカードを電子保存装置1のICカードリーダー/ライター16に挿入する(S25)。

【0033】電子保存装置1は、続いて、保存装置側外部認証鍵、ユーザ側内部認証鍵を生成すると共に(S26)、ユーザ側外部認証鍵、保存装置側内部認証鍵を生成する(S27)。つぎに、電子保存装置1は、四つの認証鍵、アカウント名等をまとめてユーザ情報とし、ユーザ情報をアカウント管理ファイルに登録する(S28)。なお、アカウント管理ファイルは、図1に示した内部記憶媒体15に記録されるものであって、例えば図3に示すような内容のものである。また、図3中に示す認証鍵情報および日時情報の内容がそれぞれ図4および図5に示されている。なお、図5に示す日時情報は、アカウント管理ファイルだけでなく、後述する各種ファイルにも含まれるものである。

【0034】ここで、認証に使用される暗号アルゴリズムが秘密鍵暗号方式の場合には、保存装置側外部認証鍵とユーザ側内部認証鍵が同じ鍵となり、ユーザ側外部認証鍵と保存装置側内部認証鍵が同じ鍵となる。その一方、暗号アルゴリズムに公開鍵暗号方式を利用する場合には、保存装置側外部認証鍵とユーザ側内部認証鍵が対応するパブリックキーとプライベートキーとなり、ユーザ側外部認証鍵と保存装置側内部認証鍵が対応するパブリックキーとプライベートキーとなる。すなわち、外部認証鍵はパブリックキーに、内部認証鍵はプライベートキーになる。

【0035】図2のフローチャートの説明に戻り、電子保存装置1は、ユーザ側内部認証鍵、ユーザ側外部認証鍵およびアカウント名をICカードに設定し(S29)、その後、ICカードをICカードリーダー/ライター16から排出し(S30)、ユーザ登録処理を終了する。一方、図2(a)に示すように、クライアント側においては、ステップS17で要求したユーザ登録要求が成功したか否かを判定し(S18)、要求が成功しなかった場合(S18; No)にはエラーとしてユーザ登録処理を終了し、要求が成功した場合(S18; Yes)には正常にユーザ登録処理を終了する。

【0036】なお、新しいICカードには予めユーザパスワードが初期値として設定されている。初期値のパスワードを照合すると任意のパスワードに変更することが可能である。パスワード変更は、電子保存装置1とは関係なく、クライアント側で行うことができる。

【0037】(2) 電子保存装置へのログイン処理  
電子保存装置1にファイルを保存したり、電子保存装置1からファイルを読み出す前に、ユーザは電子保存装置1にログインしなければならない。ログイン処理においては、ユーザ登録の際に発行されたICカードを利用し、電子保存装置1との間で相互認証が行われる。ここでは、相互認証の方法として、公知の技術を採用することにする。

【0038】図6は、電子保存装置1へのログイン処理を示すフローチャートであり、図6(a)はクライアント側で実行されるログイン処理であり、図6(b)は電子保存装置1側で実行されるログイン処理である。図6(a)において、ログインユーザ用ICカードをクライアントのカードリーダーに挿入し(S31)、パスワードを入力する(S32)。

【0039】ICカードでパスワード照合が行われ(S33)、正しいパスワードであるか否か、換言すれば、パスワードが不正でないか否かが判定される(S34)。パスワードが不正であると判定された場合(S34; No)、ログイン処理がエラーにより終了する。一方、パスワードは不正ではないと判定された場合(S34; Yes)、図6(a)および図6(b)にそれぞれ示すように、電子保存装置1およびICカードとの間で相互認証処理が実行される(S35, S41)。なお、相互認証処理については後にフローチャートを用いて説明する。

【0040】そして、相互認証処理に失敗した場合(S36, S42; No)、ログイン処理がエラーにより終了する。一方、相互認証処理に成功した場合(S36, S42; Yes)、電子保存装置1は乱数を生成し、生成した乱数をクライアントに送信し(S43)、クライアントは電子保存装置1から送信された乱数を受信する(S37)。

【0041】クライアントは、受信した乱数をICカー

ドに渡し、ユーザ側内部認証鍵で暗号化し（S38）、暗号化乱数を電子保存装置1とのセッション鍵とする（S39）。一方、電子保存装置1は、乱数をユーザ側内部認証鍵で暗号化し（S44）、暗号化乱数をクライアントとのセッション鍵とする（S45）。

【0042】その後、クライアントは、暗号処理、メッセージ認証処理モードを送信し（S40）、電子保存装置1は、暗号処理、メッセージ認証処理モードを受信し（S46）、ログイン処理を正常に終了する。

【0043】なお、クライアント側および電子保存装置1側のいずれとも、送信するデータにはセッション鍵を用いて生成したメッセージ認証子を付加し、また、受信したデータは同じくセッション鍵を用いてメッセージ認証子の検証処理を行う。また、クライアントから暗号処理モードを設定することが可能であり、暗号処理を行うように指定した場合には、クライアント側、電子保存装置1側とも、送信するデータをセッション鍵で暗号化し、また、受信したデータは同じくセッション鍵で復号する。

【0044】図7は、図6（a）のステップS35および図6（b）のステップS41において実行される相互認証処理のフローチャートであり、図7（a）はクライアント側で実行される相互認証処理を、図7（b）は電子保存装置1側で実行される相互認証処理をそれぞれ示している。

【0045】クライアントは、ICカードからアカウント名を読み出し（S51）、読み出したアカウント名を電子保存装置1に送信する（S52）。電子保存装置1は、アカウント名を受信し（S61）、アカウント管理ファイルを読み出す（S62）。そして、電子保存装置1は、読み出したアカウント管理ファイルのアカウント管理データから該当するアカウント情報を取得する処理を行う（S63）。ここで、該当するアカウント情報がアカウント管理データ中に存在しない場合（S64；No）、相互認証処理はエラーにより終了する。

【0046】一方、該当するアカウント情報がアカウント管理データ中に存在する場合（S64；Yes）、電子保存装置1は乱数1を生成し（S65）、生成した乱数1をクライアントに送信する（S66）。

【0047】クライアントは、乱数1を受信し（S53）、受信した乱数1をICカードに渡し、ユーザ側内部認証鍵で暗号化した認証コード1を取得する（S54）。続いて、クライアントは、ICカードで乱数2を生成し（S55）、認証コード1と乱数2とを電子保存装置1に送信する（S56）。

【0048】電子保存装置1は、認証コード1と乱数2とを受信し（S67）、保存装置側外部認証鍵で認証コード1を復号する（S68）。そして、電子保存装置1は、復号した認証コードと乱数1とが一致するか否かを判定する（S69）、ステップS69において、一致し

ないと判定された場合（S69；No）、相互認証処理がエラーにより終了する。一方、一致すると判定された場合（S69；Yes）、ステップS70において、電子保存装置1が乱数2を保存装置側内部認証鍵で暗号化して認証コード2を生成し（S70）、認証コード2をクライアントに送信する（S71）。

【0049】クライアントは、認証コード2を受信し（S57）、認証コード2をICカードに渡し、ユーザ側外部認証鍵により外部認証を行う（S58）。そして、外部認証が成功しなかった場合（S59；No）、相互認証処理がエラーで終了し、外部認証が成功した場合（S59；Yes）、相互認証処理が正常に終了し、図6のフローチャートの処理に戻ることになる。

【0050】（3）電子データ保存処理  
つぎに、電子データを電子保存装置1に保存する際の処理手順について説明する。図8は、電子データを電子保存装置1に保存する処理を示すフローチャートであり、図9は、原本データの保存処理の説明図である。以下では、図8のフローチャートに示す電子データ保存処理について、図9を参照しつつ具体的に説明する。

【0051】電子保存装置1のプロセッサ11は、通信ポート12を介して計算機2から電子データの保存要求を受けた場合、大容量記憶媒体13がマウントされているか否かを判定する（S81）。ここで、大容量記憶媒体13がマウントされていないと判定した場合（S81；No）、プロセッサ11は、エラーにより電子データ保存処理を終了する。

【0052】一方、大容量記憶媒体13がマウントされていると判定した場合（S81；Yes）、通信ポート12を介してユーザ側（計算機2）から、図9に示すデータ21およびファイル属性コード22を受け取る（S82）。

【0053】そして、プロセッサ11は、受け取ったファイル属性コード22が「原本」、「仮原本」または「一般」であるか否かを判定する（S83）。ここで、ファイル属性コード22が「原本」、「仮原本」または「一般」でないと判定した場合（S83；No）、プロセッサ11は、エラーにより電子データ保存処理を終了する。

【0054】一方、ファイル属性コード22が「原本」、「仮原本」または「一般」であると判定した場合（S83；Yes）、プロセッサ11は、ファイル属性コードが「一般」か否かを判定する（S84）。ファイル属性コードが「一般」であると判定した場合（S84；Yes）、プロセッサ11は、受け取ったデータ21を大容量記憶媒体13にファイルとして保存し（S92）、電子データ保存処理を正常に終了する。

【0055】また、ファイル属性コードが「一般」でないと判定した場合（S84；No）、プロセッサ11は、タイム17から現在時刻を取得すると共に、内部記



憶媒体15から装置暗号鍵41、装置復号鍵42、最新タイミDを取得し(S85)、改ざん検知保存処理を実行してデータを大容量記憶媒体13に保存する(S86)。

【0056】図10は、ステップS86の改ざん検知保存処理を示すフローチャートである。プロセッサ11は、保存するデータ21に対してハッシュ値を計算してハッシュ値23を求め(S101)、ハッシュ値23を装置暗号鍵41で暗号化してメッセージ認証子(MAC)24を生成する(S102)。その後、メッセージ認証子24と共にデータ21を保存ファイル25として大容量記憶媒体13に保存する(S103)。

【0057】図8のフローチャートに戻り、プロセッサ11は、ファイル属性コード22に対して現在時刻、ユーザアカウント名、ファイルアクセス履歴等を加えたファイル属性情報26を生成し(S87)、図10に示したような改ざん検知保存処理を実行して、ファイル属性情報26を大容量記憶媒体13に保存する(S88)。

【0058】このステップS88において実行される改ざん検知保存処理を図9および図10を参照して説明する。プロセッサ11は、図8のステップS87で生成したファイル属性情報26に対してハッシュ値を計算してハッシュ値27を求め(S101)、ハッシュ値27を装置暗号鍵41で暗号化してメッセージ認証子(MAC)28を生成する(S102)。その後、メッセージ認証子28と共にファイル属性情報26をファイル属性情報ファイル29として大容量記憶媒体13に保存する(S103)。

【0059】再び図8のフローチャートの説明に戻り、プロセッサ11は、改ざん検知読み出し処理を実行して、大容量記憶媒体13から保存ファイルリストファイル31を読み出す(S89)。

【0060】図11は、図8のステップS89において実行される改ざん検知読み出し処理を示すフローチャートである。プロセッサ11は、大容量記憶媒体13に記録されている保存ファイルリストファイル31(対象ファイル)を読み出し(S111)、保存ファイルリストファイル31に記録されている保存ファイルリスト32(データ)とメッセージ認証子(リストMAC)31とを分離する(S112)。プロセッサ11は、ステップS112で分離した保存ファイルリスト32に対してハッシュ値を計算する(S113)。

【0061】続いて、プロセッサ11は、内部記憶媒体15から装置復号鍵42を取得し(S114)、取得した装置復号鍵42でメッセージ認証子33を復号して検証用ハッシュ値を求める(S115)。プロセッサ11は、その後、ステップS113で求めたハッシュ値とステップS115で求めた検証用ハッシュ値とが一致するか否かを判定する(S116)。

【0062】ステップS116において、二つのハッ

シ値が一致しないと判定した場合(S116; No)、図8には詳細に示されていないが、プロセッサ11はエラーとして改ざん検知読み出し処理および電子データ保存処理を終了する。一方、二つのハッシュ値が一致すると判定した場合(S116; Yes)、プロセッサ11は、保存ファイルリスト32を読み出しデータとし(S117)、図8のステップS90に進む。

【0063】再び図8のフローチャートの説明に戻り、プロセッサ11は、読み出した保存ファイルリスト32に保存ファイル25のエントリを追加する(S90)。そして、プロセッサ11は、改ざん検知保存処理を実行して、保存ファイルリスト32を大容量記憶媒体13に記録し(S91)、電子データ保存処理を終了する。

【0064】なお、ステップS91において実行される改ざん検知保存処理を図9および図10を参照して説明する。プロセッサ11は、S90で保存ファイル25のエントリが追加された保存ファイルリスト32に対してハッシュ値を計算してリストハッシュ値34を求め(S101)、リストハッシュ値34を装置暗号鍵41で暗号化してメッセージ認証子(リストMAC)33を生成する(S102)。その後、メッセージ認証子33と共に保存ファイルリスト32を保存ファイルリストファイル31として大容量記憶媒体13に保存する(S103)。

【0065】なお、図9に示した各種情報の内容について簡単に示すことにする。図12は保存ファイル25の内容を示す説明図であり、図13はファイル属性情報ファイル29の内容を示す説明図であり、図14は保存ファイルリストファイル31の内容を示す説明図であり、図15はタイマ設定履歴ファイル43の内容を示す説明図である。また、図9の内部記憶媒体15に示すアカウント管理ファイル44は図3に示したものに該当する。

【0066】また、ここで、電子保存装置1における日時の管理について説明する。図13に示したファイル属性情報ファイル29中のファイルアクセス履歴等に記録する日時は、電子保存装置1内部のタイマ17から取得するものであるが、ここではタイマ17の設定を変更することができるようになっているものとする。そのため、タイマ17を不正に変更することによりファイルアクセス日時を偽ることを防止するため、タイマ17の設定を変更した履歴を記録するようにしている。タイマ17の設定を変更すると、概念的には図16に示すような履歴が内部記憶媒体15のタイマ設定履歴ファイル43に記録される。

【0067】タイミDは、電子保存装置1内部で自動的に振られるシーケンシャルな番号であり、タイマ17の設定を変更するたびに番号が増えていく。なお、ファイルアクセス履歴に含まれる日時情報には図5に示したようにタイミDが含まれている。

【0068】図16に示すようなタイマ設定履歴によ

り、タイマID=3において不正に1ヶ月日付をずらし、その後タイマID=4で日付を戻していることがわかるため、ファイルアクセス履歴の日時にタイマID=3の履歴がついているファイルは不正に日時を偽ろうとした可能性があることがわかる。タイマ設定履歴は内部記憶媒体15(タイマ設定履歴ファイル43)に記録されるが、ファイルアクセス履歴は各ファイルと共に大容量記憶媒体13に記録される。

【0069】後述するように、ある電子保存装置から他の電子保存装置に対してファイルを移動したり、コピーしたりすることが可能であるが、このような場合にもファイルアクセス履歴の日時に不整合が生じないよう、概念的には図17に示すようなファイルアクセス履歴を各ファイルに対して記録する。すなわち、図13に示したように、ファイルアクセス履歴はファイル属性情報ファイル29に記録される。例えば、図17において、移動先となる電子保存装置R010-0001055の日時19990217 10:13:43 ID=2が移動元の電子保存装置 R010-0001032の日時19990217 10:10:21 ID=3に相当することがわかるため、移動したファイルに不正が見つかった場合には、電子保存装置をまたいで履歴を辿ることができる。

【0070】(4) 大容量記憶媒体マウント処理  
大容量記憶媒体13が電子保存装置1から取り外し可能な場合には、大容量記憶媒体13を電子保存装置1に装着した際に、以下に説明する大容量記憶装置マウント処理を実行することにする。その際、媒体の正当性が検証される。

【0071】図18は、大容量記憶媒体マウント処理のフローチャートである。電子保存装置1のプロセッサ11は、大容量記憶媒体13が電子保存装置1に装着されると、装着された大容量記憶媒体13がフォーマット済みであるか否かを判定する(S121)。ステップS121においてフォーマット済みである場合(S121; Yes)はステップS123に進み、フォーマット済みでない場合(S121; No)は図19に示す大容量記憶媒体のフォーマット処理が実行される(S122)。

【0072】すなわち、ステップS122においては、図19に示すように、プロセッサ11が大容量記憶媒体13の初期化処理を実行し(S131)、乱数を生成する(S132)。プロセッサ11は、生成した乱数を保存ファイルリスト32の最初のエントリとして格納する(S133)。その後、プロセッサ11は、図10に示したように、保存ファイルリスト32の改ざん検知保存処理を実行し(S134)、図18のステップS123に進む。

【0073】プロセッサ11は、図11に示した処理に従って、保存ファイルリストファイル31の改ざん検知読み出し処理を実行し(S123)、正常に読み出し処

理を実行できた場合(S124; Yes)には大容量記憶媒体マウント処理を正常終了し、読み出し処理に失敗した場合(S124; No)には大容量記憶媒体マウント処理をエラーにより終了する。

【0074】(5) ファイル読み出し処理

ユーザ側からファイル読み出し要求を受けると、対象ファイルの正当性を検証し、データをユーザに対して送出する。

【0075】図20は、ファイル読み出し処理のフローチャートである。電子保存装置1のプロセッサ11は、ユーザ側からファイル読み出し要求を受けると、大容量記憶媒体13がマウントされているか否かを判定する(S141)。ここで、大容量記憶媒体13がマウントされていない場合(S141; No)、ファイル読み出し処理はエラーにより終了する。

【0076】一方、大容量記憶媒体13がマウントされている場合(S141; Yes)、プロセッサ11は、対象ファイル(保存ファイル25)に関連付けられたファイル属性情報ファイル29が存在するか否かを判定する(S142)。ファイル属性情報ファイル29が存在しないと判定した場合(S142; No)、プロセッサ11は、対象ファイルを読み出してユーザ側に送出する処理を実行し(S146)、ファイル読み出し処理を終了する。これに対し、ファイル属性情報ファイル29が存在すると判定した場合(S142; Yes)、プロセッサ11は、図11に示した処理に従い、対象ファイルの改ざん検知読み出し処理を実行する(S143)。

【0077】続いて、プロセッサ11は、改ざん検知読み出し処理で対象ファイルの読み出しに成功したか否かを判定する(S144)。ここで、読み出しに失敗した場合(S144; No)、プロセッサ11は、ファイル読み出し処理をエラーにより終了する。一方、読み出しに成功した場合(S144; Yes)、プロセッサ11は、読み出したデータをユーザ側に送出し(S145)、ファイル読み出し処理を正常に終了する。

【0078】(6) 謄本作成処理

「原本」の属性を持つ保存ファイル25に対し、外部から複製要求を受け取ると、対象ファイルとそれに関連付けられたファイル属性情報ファイル29をコピーすると共に、新しいファイル属性情報には「謄本」のファイル属性コード22を付与する。謄本ファイルの作成先が別の電子保存装置の場合には、別の電子保存装置にログインしてファイルを転送する。ログインの方法は、図6を用いて説明したような、ユーザが電子保存装置1にログインする方法と同様である。電子保存装置間でやり取りされるデータの保護についても、ユーザと電子保存装置1との間でやり取りするデータの保護の方法と同様である。データ保存処理と同様に、保存ファイルリスト32の更新も行われる。なお、ファイル転送先の電子保存装置においては、転送受け入れ処理が行われることにな

る。

【0079】図21は、謄本作成処理を示すフローチャートである。電子保存装置1のプロセッサ11は、図11に示した処理に従い、謄本を作成する対象となる対象ファイルのファイル属性情報ファイル29の改ざん検知読み出し処理を実行する(S151)。ここで、改ざん検知読み出し処理に失敗した場合(S152; No)、謄本作成処理をエラーによって終了する。

【0080】一方、改ざん検知読み出し処理に成功した場合(S152; Yes)、プロセッサ11は、読み出したファイル属性情報ファイル29からファイル属性コード22を取得する(S153)。プロセッサ11は、取得したファイル属性コード22が「原本」であるか否かを判定し(S154)、ファイル属性コードが「原本」でない場合(S154; No)、謄本作成処理をエラーによって終了する。

【0081】ファイル属性コードが「原本」である場合(S154; Yes)、プロセッサ11は、謄本の作成先が同一装置か否かを判定し(S155)、同一装置であると判定した場合(S155; Yes)には同一装置内での謄本作成処理を実行し(S156)、同一装置ではないと判定した場合(S155; No)には他の装置での謄本作成処理を実行し(S157)、謄本作成処理を終了する。

【0082】図22は、図21のステップS156において実行される同一装置内での謄本作成処理のフローチャートである。まず、プロセッサ11は、作成先のファイルが既に存在しているか否かを判定し(S161)、存在している場合(S161; Yes)にはエラーにより同一装置内での謄本作成処理を終了する。換言すれば、図21に示した謄本作成処理をエラーで終了することになる。

【0083】一方、作成先のファイルが存在していない場合(S161; No)、プロセッサ11は、対象ファイルを作成先ファイルにコピーする(S163)。そして、プロセッサ11は、対象ファイルのファイル属性情報ファイル29を作成先のファイル属性情報ファイルとしてコピーする(S163)。

【0084】続いて、プロセッサ11は、図11に示した処理に従い、作成先のファイル属性情報ファイル29の改ざん検知読み出し処理を実行し(S164)、読み出したファイル属性情報26のファイル属性コード22を「謄本」に変更する(S165)。

【0085】プロセッサ11は、タイマ17から現在時刻を取得し(S166)、ファイル属性情報26に謄本作成履歴(アカウント名、現在時刻、タイムID等)を追加し(S167)、図10に示した処理に従い、ファイル属性情報26の改ざん検知保存処理を実行する(S168)。

【0086】さらに、プロセッサ11は、保存ファイル

リストファイル31の改ざん検知読み出し処理を実行し(S169)、読み出し処理に失敗した場合(S170; No)、作成先ファイルおよび作成先ファイル属性情報ファイルを削除し(S173)、エラーにより図22の処理を終了する。すなわち、図21の謄本作成処理をエラーで終了することになる。

【0087】一方、読み出し処理に成功した場合(S170; Yes)、プロセッサ11は、保存ファイルリスト32に作成先ファイルのエントリを追加し(S171)、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して(S172)、図21の謄本作成処理を正常に終了する。

【0088】図23は、図21のステップS157において実行される他の装置での謄本作成処理のフローチャートである。プロセッサ11は、図6に示したような処理に従い、作成先保存装置へのログイン処理を実行する(S181)。ここで、ログイン処理に失敗した場合(S182; No)、プロセッサ11は図23の処理をエラーで終了する。すなわち、図21の処理がエラーで終了することになる。

【0089】一方、ログイン処理に成功した場合(S182; Yes)、プロセッサ11は、図11に示した処理に従い、対象ファイルの改ざん検知読み出し処理を実行し(S183)、読み出しデータを作成先保存装置に謄本作成モードで転送する(S184)。

【0090】続いて、プロセッサ11は、図11に示した処理に従い、対象ファイルのファイル属性情報ファイル29の改ざん検知読み出し処理を実行する(S185)。そして、プロセッサ11は、タイマ17から現在時刻を取得し(S186)、ファイル属性情報26に謄本作成履歴を追加する(S187)。

【0091】そして、プロセッサ11は、ファイル属性情報26を作成先保存装置に謄本作成モードで転送し(S188)、転送が成功した場合には(S189; Yes)、作成先保存装置からログアウトし(S190)、図21に示す謄本作成処理を終了する。一方、転送に失敗した場合(S189; No)、図23の処理をエラーで終了する。すなわち、図21の謄本作成処理もエラーで終了ということになる。

【0092】図24は、図23に示す他の装置での謄本作成処理が実行された場合に、他の装置、即ち図23に示した作成先保存装置で行われる転送受け入れ処理(謄本作成モード)を示すフローチャートである。作成先保存装置は、転送先ファイルが既に存在しているか否かを判定し(S191)、転送先ファイルが既に存在している場合(S191; Yes)にはエラーで図24の処理を終了する。この場合、図21の謄本作成処理もエラーで終了ということになる。

【0093】また、作成先保存装置は、転送先ファイルが存在しないと判定した場合(S191; No)、図1

1に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する(S192)。ここで、改ざん検知読み出し処理に失敗した場合(S193; No)、エラーにより図24の処理を終了する。一方、読み出しに成功した場合(S193; Yes)、作成先保存装置は、図10に示した処理に従い、受け取ったデータの改ざん検知保存処理を実行する(S194)。

【0094】続いて、作成先保存装置は、受け取ったファイル属性情報26のファイル属性コード22を「謄本」に変更し(S195)、ファイル属性情報26に謄本作成履歴を追加して(S196)、図10に示した処理に従ってファイル属性情報26の改ざん検知保存処理を実行する(S197)。

【0095】その後、作成先保存装置は、保存ファイルリスト32に作成した謄本ファイルのエントリを追加し(S198)、図10に示した処理に従い、保存ファイルリスト32の改ざん検知保存処理を実行し(S199)、図24の処理を終了する。

【0096】(7)バックアップ作成処理  
「仮原本」、「原本」、「謄本」の属性を持つファイルに対して外部からバックアップ作成要求を受け取ると、対象ファイルと、それに関連付けられたファイル属性情報ファイルをコピーし、新しいファイル属性ファイルには元のファイル属性コードに対応する「バックアップ仮原本」、「バックアップ原本」、「バックアップ謄本」というファイル属性コードをつけることにする。バックアップファイルの作成先が別の電子保存装置の場合には、その別の電子保存装置にログインしてファイルを転送する。データ保存処理と同様に、保存ファイルリストの更新も行う。なお、ファイル転送先の電子保存装置では、転送受け入れ処理が行われることになる。

【0097】図25は、バックアップ作成処理のフローチャートである。電子保存装置1のプロセッサ11は、バックアップの作成対象となる対象ファイルのファイル属性情報ファイル29の改ざん検知読み出し処理を実行する(S201)。ここで、改ざん検知読み出し処理による読み出しに失敗した場合(S202; No)、エラーによりバックアップ作成処理を終了する。

【0098】一方、読み出しに成功した場合(S202; Yes)、読み出したファイル属性情報ファイル29からファイル属性コード22を取得する(S203)。そして、プロセッサ11は、バックアップ作成先が同一装置か否かを判定し(S204)、同一装置と判定した場合(S204; Yes)には同一装置内でのバックアップ作成処理を実行し(S205)、同一装置ではないと判定した場合(S204; No)には他の装置でのバックアップ作成処理を実行し(S206)、バックアップ作成処理を終了する。

【0099】図26は、図25のステップS205にお

いて実行される同一装置内でのバックアップ作成処理のフローチャートである。プロセッサ11は、作成先のファイルが既に存在するか否かを判定し(S210)、存在する場合(S210; Yes)にはエラーとして図25および図26に示すバックアップ作成処理を終了する。一方、作成先のファイルが存在しない場合(S210; No)には対象ファイルを作成先ファイルにコピーする(S211)。

【0100】続いて、プロセッサ11は、対象ファイルのファイル属性情報ファイル29を作成先のファイル属性情報ファイルとしてコピーする(S212)。プロセッサ11は、さらに、図11に示した処理に従い、作成先のファイル属性情報ファイル29の改ざん検知読み出し処理を実行し(S213)、ファイル属性コード22を変更する処理を実行する(S214)。

【0101】具体的には、ファイル属性コードが「仮原本」の場合は「バックアップ仮原本」に変更し、「原本」の場合は「バックアップ原本」に変更し、「謄本」の場合は「バックアップ謄本」に変更する。

【0102】そして、プロセッサ11は、タイマ17から現在時刻を取得し(S215)、ファイル属性情報26にバックアップ作成履歴(アカウント名、現在時刻、タイマID等)を追加した後(S216)、図10に示した処理に従い、ファイル属性情報26の改ざん検知保存処理を実行する(S217)。

【0103】続いて、プロセッサ11は、図11に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行し(S218)、読み出しに成功した場合(S219; Yes)、保存ファイルリスト32に作成先ファイルのエントリを追加し(S220)、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して(S221)、図26の処理を終了する。

【0104】一方、保存ファイルリストファイル31の改ざん検知読み出し処理に失敗した場合(S219; No)、作成先ファイルおよび作成先ファイル属性情報ファイルを削除する処理を実行し(S222)、エラーとして図25および図26の処理を終了する。

【0105】図27は、図25のステップS206において実行される他の装置でのバックアップ作成処理のフローチャートである。電子保存装置1のプロセッサ11は、図6に示したようにして、作成先保存装置へのログイン処理を実行する(S231)。ここで、ログイン処理に成功しなかった場合(S232; No)は、エラーにより図25および図27の処理を終了し、ログイン処理に成功した場合(S232; Yes)は、図11に示した処理に従って対象ファイルの改ざん検知読み出し処理を実行する(S233)。

【0106】続いて、プロセッサ11は、読み出しデータを作成先保存装置にバックアップ作成モードで転送し

( S234 )、図11に示した処理に従い、対象ファイルのファイル属性情報ファイル29の改ざん検知読み出し処理を実行する ( S235 )。

【0107】そして、プロセッサ11は、タイマ17から現在時刻を取得し ( S236 )、ファイル属性情報26に謄本作成履歴を追加する ( S237 )。そして、プロセッサ11は、ファイル属性情報26を作成先保存装置にバックアップ作成モードで転送し ( S238 )、転送が成功した場合 ( S239 ; Yes ) には作成先保存装置からのログアウト処理を実行して ( S240 )、図27に示す処理を正常に終了する。一方、転送に失敗した場合 ( S239 )、エラーにより図25および図27に示す処理が終了する。

【0108】図28は、図27に示す他の装置でのバックアップ作成処理が実行された場合に、他の装置、即ち図27に示した作成先保存装置で行われる転送受け入れ処理 ( バックアップ作成モード ) を示すフローチャートである。作成先保存装置は、転送先ファイルが既に存在しているか否かを判定し ( S241 )、転送先ファイルが既に存在している場合 ( S241 ; Yes ) にはエラーで図28の処理を終了する。この場合、図25のバックアップ作成処理もエラーで終了ということになる。

【0109】また、作成先保存装置は、転送先ファイルが存在しないと判定した場合 ( S241 ; No )、図11に示した処理に従って、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S242 )。ここで、改ざん検知読み出し処理に失敗した場合 ( S243 ; No )、エラーにより図28の処理を終了する。一方、読み出しに成功した場合 ( S243 ; Yes )、作成先保存装置は、図10に示した処理に従って、受け取ったデータの改ざん検知保存処理を実行する ( S244 )。

【0110】続いて、作成先保存装置は、受け取ったファイル属性情報26のファイル属性コード22を値に応じて「バックアップ」に変更し ( S245 )、ファイル属性情報26にバックアップ作成履歴を追加して ( S246 )、図10に示した処理に従ってファイル属性情報26の改ざん検知保存処理を実行する ( S247 )。

【0111】その後、作成先保存装置は、保存ファイルリスト32に作成したバックアップファイルのエントリを追加し ( S248 )、図10に示した処理に従って、保存ファイルリスト32の改ざん検知保存処理を実行し ( S249 )、図28の処理を終了する。

【0112】( 8 ) ファイル移動処理

同一の電子保存装置1内または別の電子保存装置1へファイルを移動する際には、このファイル移動処理が実行される。ファイルの移動先が別の電子保存装置1の場合、移動先の電子保存装置1においては、転送受け入れ処理が実行される。

【0113】図29は、ファイル移動処理を示すフロー

チャートである。電子保存装置1のプロセッサ11は、ファイルの移動処理の実行が指定されると、移動先が同一装置内であるか否かを判定し ( S251 )、移動先が同一装置内であると判定した場合 ( S251 ; Yes )、作成先のファイルが既に存在しているか否かを判定する ( S252 )。

【0114】ステップS252において、作成先のファイルが既に存在していると判定した場合 ( S252 ; Yes )、プロセッサ11は、エラーとしてファイル移動処理を終了する。一方、作成先のファイルが存在しないと判定した場合 ( S252 ; No )、プロセッサ11は、図11に示した処理に基づいて、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S253 )。そして、プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S254 ; No )、エラーとしてファイル移動処理を終了する。一方、改ざん検知読み出し処理が成功した場合 ( S254 ; Yes )、対象ファイル ( 保存ファイル25 ) を移動先ファイルに移動する ( S255 )。

【0115】また、プロセッサ11は、対象ファイルにファイル属性情報ファイル29が存在しているか否かを判定し ( S256 )、存在していないと判定した場合 ( S256 ; No ) にはステップS258に進み、存在していると判定した場合 ( S256 ; Yes ) には、ファイル属性情報ファイル29を移動先のファイル属性情報ファイルとして移動する ( S257 )。

【0116】そして、プロセッサ11は、保存ファイルリスト32内の移動したファイルのエントリを更新し ( S258 )、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行し ( S259 )、ファイル移動処理を終了する。

【0117】さらに、プロセッサ11は、ステップS251において移動先が同一装置内ではないと判定した場合 ( S251 ; No )、他の装置へのファイル移動処理を実行する ( S260 )。

【0118】図30は、図29のステップS260において実行される他の装置へのファイル移動処理を示すフローチャートである。電子保存装置1のプロセッサ11は、図11に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S261 )。プロセッサ11は、改ざん検知読み出し処理に失敗した場合に ( S262 ; No )、エラーとして図30および図29のファイル移動処理を終了し、改ざん検知読み出し処理に成功した場合 ( S262 ; Yes )、移動先保存装置へのログイン処理を実行する ( S263 )。

【0119】プロセッサ11は、ログイン処理に失敗した場合 ( S264 ; No )、エラーとして図30および図29のファイル移動処理を終了し、ログイン処理に成功した場合 ( S264 ; Yes )、図11に示した処理

に従って、移動するファイルとして指定された保存ファイル25、即ち対象ファイルの改ざん検知読み出し処理を実行し ( S265 )、読み出しデータを移動先保存装置に移動モードで転送する ( S266 )。プロセッサ11は、転送に失敗した場合 ( S267 ; No )、エラーとして図30および図29のファイル移動処理を終了し、転送に成功した場合 ( S267 ; Yes )、対象ファイルにファイル属性情報ファイル29が存在しているか否かを判定する ( S268 )。ファイル属性情報ファイル29が存在していないと判定した場合は ( S268 ; No )、ステップS274に進む。

【0120】一方、ファイル属性情報ファイル29が存在していると判定した場合 ( S268 ; Yes )、プロセッサ11は、図11に示した処理に従って、ファイル属性情報ファイル29の改ざん検知読み出し処理を実行する ( S269 )。そして、プロセッサ11は、タイマ17から現在時刻を取得し ( S270 )、ファイル属性情報26にファイル移動履歴を追加する ( S271 )。その後、プロセッサ11は、ファイル属性情報26を移動先保存装置に移動モードで転送する ( S272 )。

【0121】続いて、プロセッサ11は、転送に失敗した場合 ( S273 ; No )、エラーとして図30および図29のファイル移動処理を終了し、転送に成功した場合 ( S273 ; Yes )、対象ファイルの削除 ( S274 )、対象ファイルのファイル属性情報ファイル29の削除 ( S275 )、保存ファイルリスト32内に存在する移動したファイルのエントリの削除 ( S276 )、図10に示した処理に基づく保存ファイルリスト32の改ざん検知保存処理 ( S277 ) および作成先保存装置からのログアウト処理 ( S278 ) を順次実行して図30および図29のファイル移動処理を終了する。

【0122】図31は、図30に示す他の装置へのファイル移動処理が実行された場合に、他の装置、即ち図30に示した移動先保存装置で行われる転送受け入れ処理 ( 移動モード ) を示すフローチャートである。移動先保存装置は、転送先ファイルが既に存在しているか否かを判定し ( S281 )、転送先ファイルが存在していると判定した場合 ( S281 ; Yes )、エラーとして転送受け入れ処理を終了する。

【0123】一方、転送先ファイルが存在していないと判定した場合 ( S281 ; No )、移動先保存装置は、図11に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S282 )。移動先保存装置は、改ざん検知読み出し処理に失敗した場合 ( S283 ; No )、エラーとして転送受け入れ処理を終了し、改ざん検知読み出し処理に成功した場合 ( S283 ; Yes )、図10に示した処理に従って、受け取ったデータの改ざん検知保存処理を実行する ( S284 )。

【0124】さらに、移動先保存装置は、ファイル属性

情報26を受け取ったか否かを判定し ( S285 )、受け取っていない場合には ( S285 ; No ) そのまま処理を終了し、受け取った場合には ( S285 ; Yes ) ファイル属性情報26にファイル移動履歴を追加する ( S286 )。

【0125】そして、移動先保存装置は、図10に示した処理に従ってファイル属性情報26の改ざん検知保存処理を実行し ( S287 )、保存ファイルリスト32に受け取ったファイルのエントリを追加し ( S288 )、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して ( S289 )、転送受け入れ処理を終了する。

【0126】( 9 ) ファイル削除処理

保存ファイル25を削除するための処理である。しかし、「原本」のファイル属性コード22を有する保存ファイル25については証拠隠滅を防ぐために削除は禁止される。

【0127】図32は、ファイル削除処理を示すフローチャートである。電子保存装置1のプロセッサ11は、ファイルの削除が指定されると、大容量記憶媒体13がマウントされているか否かを判定し ( S291 )、マウントされていないと判定した場合 ( S291 ; No )、エラーとしてファイル削除処理を終了する。一方、マウントされていると判定した場合 ( S291 ; Yes )、削除が指定された保存ファイル25、即ち対象ファイルに対応するファイル属性情報ファイル29が存在するか否かを判定する ( S292 )。

【0128】プロセッサ11は、ファイル属性情報ファイル29が存在しないと判定した場合 ( S292 ; No )、対象ファイルを削除し ( S302 )、ファイル削除処理を終了する。一方、ファイル属性情報ファイル29が存在すると判定した場合 ( S292 ; Yes )、図11に示した処理に従って、対象ファイルに対応するファイル属性情報ファイル29の改ざん検知読み出し処理を実行する ( S293 )。

【0129】そして、プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S294 ; No )、エラーとしてファイル削除処理を終了し、改ざん検知読み出し処理に成功した場合 ( S294 ; Yes )、ファイル属性情報26に含まれるファイル属性コード22が「原本」であるか否かを判定する ( S295 )。

【0130】ファイル属性コード22が「原本」であると判定した場合 ( S295 ; Yes )、原本の削除は禁止されているため、プロセッサ11はエラーとしてファイル削除処理を終了する。一方、「原本」ではないと判定した場合 ( S295 ; No )、プロセッサ11は、対象ファイルを削除し ( S296 )、さらに、ファイル属性情報ファイル29を削除する ( S297 )。

【0131】続いて、プロセッサ11は、図11に示した処理に従って、保存ファイルリストファイル31の改

ざん検知読み出し処理を実行する ( S298 )。プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S299 ; No )、エラーとしてファイル削除処理を終了し、改ざん検知読み出し処理に成功した場合 ( S299 ; Yes )、保存ファイルリスト32から対象ファイルのエントリを削除し ( S300 )、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して ( S301 )、ファイル削除処理を終了する。

【0132】(10) ファイル属性コード変更処理  
データ保存処理において、「仮原本」の属性を持つファイルを保存することが可能であるが、この「仮原本」ファイルは単純にファイル属性コード22を「原本」に変更することが可能なものである。また、「謄本」、「バックアップ仮原本」、「バックアップ原本」および「バックアップ謄本」の属性を持つファイルは、それぞれファイル属性コード22を変更することで元のファイルを復旧するために利用することができる。復旧すると、ファイル属性コードは図33に示すようになる。

【0133】ファイル属性コード22の変更は、ファイルアクセス履歴として記録される。このファイル属性コード変更処理は、外部からのファイル属性コード22の変更要求と共に、新しいファイル属性コード22を受け取ることによって実行される。

【0134】図34は、ファイル属性コード変更処理を示すフローチャートである。電子保存装置1のプロセッサ11は、ファイル属性コード変更処理の指示があると、大容量記憶媒体13がマウントされているか否かを判定する ( S310 )。プロセッサ11は、大容量記憶媒体13がマウントされていないと判定した場合 ( S310 ; No )、エラーとしてファイル属性コード変更処理を終了し、大容量記憶媒体13がマウントされていると判定した場合 ( S310 ; Yes )、変更対象の保存ファイル25、即ち対象ファイルに対応するファイル属性情報ファイル29が存在しているか否かを判定する ( S311 )。

【0135】プロセッサ11は、ファイル属性情報ファイル29が存在しないと判定した場合 ( S311 ; No )、エラーとしてファイル属性コード変更処理を終了し、存在すると判定した場合 ( S311 ; Yes )、図11に示す処理に従ってファイル属性情報ファイル29の改ざん検知読み出し処理を実行する ( S312 )。プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S313 ; No )、エラーとしてファイル属性コード変更処理を終了し、改ざん検知読み出し処理に成功した場合 ( S313 ; Yes )、指定された新ファイル属性コードに応じたコード変更処理を実行する ( S314 )。

【0136】図35 ( a ) ~ 図35 ( c ) は、図34のステップS314において実行されるコード変更処理の

フローチャートである。図35 ( a ) は新ファイル属性コードとして「仮原本」が指定された場合であり、プロセッサ11は、現在のファイル属性コード22が「バックアップ仮原本」であるか否かを判定する ( S331 )。現在のファイル属性コード22が「バックアップ仮原本」ではない場合 ( S331 ; No )、エラーとして図35および図34のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード22が「バックアップ仮原本」である場合 ( S331 ; Yes )、ファイル属性情報26のファイル属性コード22を「仮原本」に変更する処理を実行する ( S332 )。

【0137】また、図35 ( b ) は新ファイル属性コードとして「原本」が指定された場合であり、プロセッサ11は、現在のファイル属性コード22が「バックアップ原本」または「仮原本」であるか否かを判定する ( S341 )。現在のファイル属性コード22が「バックアップ原本」または「仮原本」ではない場合 ( S341 ; No )、エラーとして図35および図34のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード22が「バックアップ原本」または「仮原本」である場合 ( S341 ; Yes )、ファイル属性情報26のファイル属性コード22を「原本」に変更する処理を実行する ( S342 )。

【0138】さらに、図35 ( c ) は新ファイル属性コードとして「謄本」が指定された場合であり、プロセッサ11は、現在のファイル属性コード22が「バックアップ謄本」であるか否かを判定する ( S351 )。現在のファイル属性コード22が「バックアップ謄本」ではない場合 ( S351 ; No )、エラーとして図35および図34のファイル属性コード変更処理を終了する。一方、現在のファイル属性コード22が「バックアップ謄本」である場合 ( S351 ; Yes )、ファイル属性情報26のファイル属性コード22を「謄本」に変更する処理を実行する ( S352 )。

【0139】図34のフローチャートの説明に戻り、プロセッサ11は、図35を用いて説明したステップS314においてコード変更処理を行った後、タイム17から現在時刻を取得し ( S315 )、ファイル属性情報26にファイル属性コード変更履歴を追加する ( S316 )。

【0140】続いて、プロセッサ11は、図10に示した処理に従ってファイル属性情報26の改ざん検知保存処理を行い ( S317 )、図11に示した処理に従って保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S318 )。そして、プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S319 ; No )、エラーとしてファイル属性コード変更処理を終了する。一方、改ざん検知読み出し処理に成功した場合 ( S319 ; Yes )、プロセッサ11は、保存ファイルリスト32の対象ファイルのエントリについて内

容を更新し ( S320 )、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して ( S321 )、ファイル属性コード変更処理を終了する。

#### 【0141】(11) ファイル追記処理

「原本」や「仮原本」のファイル属性コード22を持つファイルに対しては、編集は許可しないが追記は可能とする。追記のみを許可することにより、以前のデータが失われず、電子データの編集履歴がわかるため、その証明力も高まることになる。また、「謄本」およびバックアップのファイルについては追記も編集も許可しない。これは、データの訂正や修正は原本に対して施すべきものであって、コピーである謄本に施すべきものではないという考えに基づくものである。なお、ファイルの最終更新日時が変更されるため、データ保存処理と同様に保存ファイルリスト32についても更新されることになる。

【0142】図36は、ファイル追記処理を示すフローチャートである。電子保存装置1のプロセッサ11は、大容量記憶媒体13がマウントされているか否かを判定し ( S361 )、マウントされていない場合 ( S361 ; No )、エラーとしてファイル追記処理を終了する。

【0143】一方、大容量記憶媒体13がマウントされていると判定した場合 ( S361 ; Yes )、プロセッサ11は、追記処理の対象となる保存ファイル25、即ち対象ファイルに対応するファイル属性情報ファイル29が存在するか否かを判定する ( S362 )。プロセッサ11は、ファイル属性情報ファイル29が存在しないと判定した場合 ( S362 ; No )、対象ファイルにデータを追記する処理を実行し ( S374 )、ファイル追記処理を終了する。一方、ファイル属性情報ファイル29が存在すると判定した場合 ( S362 ; Yes )、プロセッサ11は、図11に示した処理に従い、ファイル属性情報ファイル29の改ざん検知読み出し処理を実行する ( S363 )。

【0144】そして、プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S364 ; No )、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成功した場合 ( S364 ; Yes )、ファイル属性コード22が「原本」または「仮原本」であるか否かを判定する ( S365 )。「原本」または「仮原本」でない場合 ( S365 ; No )、エラーとしてファイル追記処理を終了し、「原本」または「仮原本」である場合 ( S365 ; Yes )、図11に示した処理に従って、対象ファイルの改ざん検知読み出し処理を実行する ( S366 )。

【0145】プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S367 ; No )、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成

功した場合 ( S367 ; Yes )、図11に示した処理に従い、保存ファイルリストファイル31の改ざん検知読み出し処理を実行する ( S368 )。

【0146】プロセッサ11は、改ざん検知読み出し処理に失敗した場合 ( S369 ; No )、エラーとしてファイル追記処理を終了し、改ざん検知読み出し処理に成功した場合 ( S369 ; Yes )、読み出しデータに追記データを追加する処理を実行する ( S370 )。

【0147】そして、プロセッサ11は、図10に示した処理に従って追記済みデータの改ざん検知保存処理を実行し ( S371 )、保存ファイルリスト32中の対象ファイルのエントリを更新し ( S372 )、さらに、図10に示した処理に従って保存ファイルリスト32の改ざん検知保存処理を実行して ( S373 )、ファイル追記処理を終了する。

#### 【0148】(12) ファイル編集処理

「仮原本」や「原本」ファイルについては修正履歴を残すことで証明力を高めるため、これらのファイルに対する編集要求については拒否するものとする。また、「謄本」ファイルやバックアップファイルは、本来編集すべき対象ではないため、これらのファイルに対する編集要求についても拒否することにする。したがって、ここでは「一般」ファイルのみ編集可能とする。

【0149】図37は、ファイル編集処理を示すフローチャートである。電子保存装置1のプロセッサ11は、大容量記憶媒体13がマウントされているか否かを判定し ( S381 )、マウントされていない場合 ( S381 ; No )、エラーとしてファイル編集処理を終了する。

【0150】一方、大容量記憶媒体13がマウントされていると判定した場合 ( S381 ; Yes )、プロセッサ11は、編集対象として指定された保存ファイル25、即ち対象ファイルにファイル属性情報ファイル29が存在しているか否かを判定する ( S382 )。ファイル属性情報ファイル29が存在している場合 ( S382 ; Yes )、そのファイルは「一般」ファイルではないため、エラーとしてファイル編集処理を終了する。一方、ファイル属性情報ファイル29が存在していない場合 ( S382 ; No )、プロセッサ11は、対象ファイルの編集処理を実行し ( S383 )、ファイル編集処理を終了する。

【0151】このように、本実施の形態に係る原本性保証電子保存方法によれば、電子データの改ざんを防止することに加えて、紙の原本が有する性質を電子情報に持たせることを可能とすることにより、電子情報の証明力を高めることができる。

【0152】以上説明した本実施の形態に係る原本性保証電子保存方法は、予め用意されたプログラムを図1に示したような電子保存装置1 ( コンピュータ ) で実行することによって実現することが可能である。換言すれ



ば、このようなプログラムを電子保存装置1（コンピュータ）で実行することにより、例えばファイル管理システムと同じローカルネットワーク上に存在する原本性保証サーバを実現することが可能となる。

【0153】また、上記プログラムを、図1に示した電子保存装置1に予めインストールして提供することにしても良いし、フロッピーディスク、CD-ROM、MO、DVD等のコンピュータで読み取り可能な記録媒体に記録して提供することにしても良い。加えて、上記プログラムを、ネットワークや放送波等を介して提供することもできる。

【0154】

【発明の効果】以上説明したように、本発明の原本性保証電子保存方法（請求項1）によれば、電子データを保存する際に、少なくとも原本の電子データとその他の電子データとを識別可能な状態で保存し、原本の電子データに対するアクセス制御のレベルおよびその他の電子データに対するアクセス制御のレベルを制御するため、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能となる。

【0155】また、本発明の原本性保証電子保存方法（請求項2）によれば、電子データが対応する属性情報と共に保存され、属性情報がユーザによる編集入力を行えないように管理されており、原本の電子データに対し、属性情報として原本であることを示す属性コードを付与するため、紙の原本が有する性質を電子情報に持たせることが可能となる。

【0156】また、本発明の原本性保証電子保存方法（請求項3）によれば、さらに、原本の電子データに対する修正履歴を記録することにしたため、電子情報の証明力を高めることが可能となる。

【0157】また、本発明の原本性保証電子保存方法（請求項4）によれば、さらに、原本の電子データに対する削除処理の実行を禁止することにしたため、電子情報の証明力を高めることが可能となる。

【0158】また、本発明の原本性保証電子保存方法（請求項5）によれば、さらに、原本の電子データの複製を生成し、生成した複製を原本に対する謄本として管理するようしたため、紙が有する性質を電子情報に持たせることができる。

【0159】また、本発明の原本性保証電子保存方法（請求項6）によれば、さらに、原本の電子データの作成もしくは修正した順番または時刻に関する情報を、外部から変更できないようにするか、または変更されても変更された事実を検出可能な状態で、原本の電子データと共に保存するため、電子情報の証明力を高めることが可能となる。

【0160】また、本発明の原本性保証電子保存方法（請求項7）によれば、さらに、電子データの移動が要求された場合に、電子データを対応する属性情報と共に

移動させることにしたため、移動先においても移動元と同様に、電子データに対するアクセス制御のレベルを制御することが可能となる。

【0161】また、本発明の原本性保証電子保存方法（請求項8）によれば、さらに、原本または謄本の電子データおよび対応する属性情報にメッセージ認証子を付与して保存し、電子データがアクセスされた場合に、メッセージ認証子を用いて電子データに対する改ざんを検出するため、電子情報の証明力を高めることが可能となる。

【0162】また、本発明の原本性保証電子保存方法（請求項9）によれば、さらに、第1の保存装置に存在する電子データの複製を第2の保存装置に生成するための要求または第1の保存装置に存在する電子データを第2の保存装置に移動させるための要求があった場合に、第1の保存装置が、電子データおよび対応する属性情報のそれぞれに付与されたメッセージ認証子を検証した後、メッセージ認証子を除いた電子データおよび対応する属性情報を第2の保存装置に転送し、第2の保存装置が、電子データおよび対応する属性情報を受け取り、処理内容に応じて属性情報を変更し、電子データおよび対応する属性情報に対してメッセージ認証子を付与して保存するため、紙の原本が有する性質を電子情報に持たせ、電子情報の証明力を高めることが可能となる。

【0163】さらに、本発明のコンピュータ読み取り可能な記録媒体（請求項10）によれば、請求項1～9のいずれか一つに記載の原本性保証電子保存方法をコンピュータに実行させるためのプログラムを記録したことにより、このプログラムをコンピュータに実行させることにより、例えばユーザサイトに設置可能な原本性保証機能を有する認証サーバを実現することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る原本性保証電子保存方法を実行する電子保存装置のブロック構成図である。

【図2】本発明の実施の形態に係るユーザ登録処理を示すフローチャートであり、(a)はクライアント側で実行されるユーザ登録処理を、(b)は電子保存装置側で実行されるユーザ登録処理をそれぞれ示している。

【図3】図2(b)のステップS28で用いられるアカウント管理ファイルの内容を示す説明図である。

【図4】図3に示す認証鍵情報の内容を示す説明図である。

【図5】図3中に示す日時情報の内容を示す説明図である。

【図6】本発明の実施の形態に係る電子保存装置へのログイン処理を示すフローチャートであり、(a)はクライアント側で実行されるログイン処理を、(b)は電子保存装置側で実行されるログイン処理をそれぞれ示している。

【図7】図6(a)のステップS35および図6(b)

のステップS41において実行される相互認証処理のフローチャートであり、(a)はクライアント側で実行される相互認証処理を、(b)は電子保存装置側で実行される相互認証処理をそれぞれ示している。

【図8】本発明の実施の形態に係る電子データ保存処理を示すフローチャートである。

【図9】図8に示す電子データ保存処理において、原本データを保存する際の処理の説明図である。

【図10】本発明の実施の形態に係る改ざん検知保存処理を示すフローチャートである。

【図11】本発明の実施の形態に係る改ざん検知読み出し処理を示すフローチャートである。

【図12】図9に示す保存ファイルの説明図である。

【図13】図9に示すファイル属性情報ファイルの説明図である。

【図14】図9に示す保存ファイルリストファイルの説明図である。

【図15】図9に示すタイマ設定履歴ファイルの説明図である。

【図16】図15に示すタイマ設定履歴ファイル中のタイマ設定履歴の説明図である。

【図17】図13に示すファイル属性情報ファイル中のアクセス履歴の説明図である。

【図18】本発明の実施の形態に係る大容量記憶媒体マウント処理のフローチャートである。

【図19】図19のステップS122で実行される大容量記憶媒体のフォーマット処理を示すフローチャートである。

【図20】本発明の実施の形態に係るファイル読み出し処理のフローチャートである。

【図21】本発明の実施の形態に係る謄本作成処理を示すフローチャートである。

【図22】図21のステップS156において実行される同一装置内での謄本作成処理のフローチャートである。

【図23】図21のステップS157において実行される他の装置での謄本作成処理のフローチャートである。

【図24】図23に示す他の装置での謄本作成処理が実行された場合に、他の装置で行われる転送受け入れ処理（謄本作成モード）を示すフローチャートである。

【図25】本発明の実施の形態に係るバックアップ作成処理のフローチャートである。

【図26】図25のステップS205において実行される同一装置内でのバックアップ作成処理のフローチャートである。

【図27】図25のステップS206において実行される他の装置でのバックアップ作成処理のフローチャートである。

【図28】図27に示す他の装置でのバックアップ作成

処理が実行された場合に、他の装置で行われる転送受け入れ処理（バックアップ作成モード）を示すフローチャートである。

【図29】本発明の実施の形態に係るファイル移動処理を示すフローチャートである。

【図30】図29のステップS260において実行される他の装置へのファイル移動処理を示すフローチャートである。

【図31】図30に示す他の装置へのファイル移動処理が実行された場合に、他の装置で行われる転送受け入れ処理（移動モード）を示すフローチャートである。

【図32】本発明の実施の形態に係るファイル削除処理を示すフローチャートである。

【図33】本発明の実施の形態に係るファイル属性コード変更処理の説明図である。

【図34】本発明の実施の形態に係るファイル属性コード変更処理を示すフローチャートである。

【図35】図34のステップS314において実行されるコード変更処理のフローチャートである。

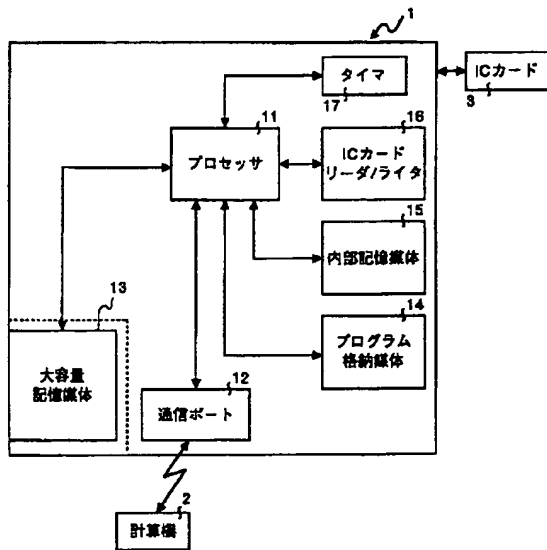
【図36】本発明の実施の形態に係るファイル追記処理を示すフローチャートである。

【図37】本発明の実施の形態に係るファイル編集処理を示すフローチャートである。

#### 【符号の説明】

- |            |               |
|------------|---------------|
| 1          | 電子保存装置        |
| 2          | 計算機（クライアント）   |
| 3          | ICカード         |
| 11         | プロセッサ         |
| 12         | 通信ポート         |
| 13         | 大容量記憶媒体       |
| 14         | プログラム格納媒体     |
| 15         | 内部記憶媒体        |
| 16         | ICカードリーダ／ライタ  |
| 17         | タイマ           |
| 21         | データ           |
| 22         | ファイル属性コード     |
| 23, 27     | ハッシュ値         |
| 24, 28, 33 | メッセージ認証子      |
| 25         | 保存ファイル        |
| 26         | ファイル属性情報      |
| 29         | ファイル属性情報ファイル  |
| 31         | 保存ファイルリストファイル |
| 32         | 保存ファイルリスト     |
| 34         | リストハッシュ値      |
| 41         | 装置暗号鍵         |
| 42         | 装置復号鍵         |
| 43         | タイマ設定履歴ファイル   |
| 44         | アカウント管理ファイル   |

【図1】



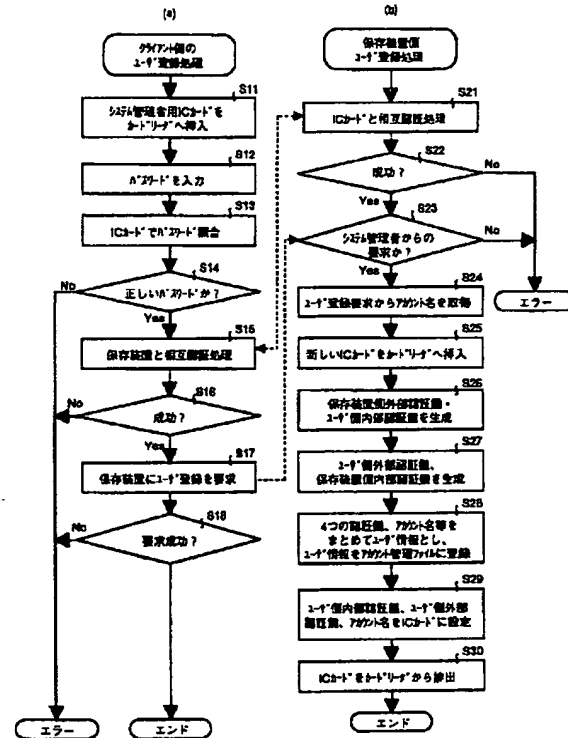
【図3】

アカウントエントリ#1	アカウント名
	アカウント登録日時情報
	アカウント抹消日時情報
	最終ログアウト日時情報
	保存装置側外部認証情報
	ユーザ側内部認証情報
	ユーザ側外部認証情報
	保存装置側内部認証情報
	登録抹消フラグ
	使用済みフラグ
アカウントエントリ#2	
アカウントエントリ#3	

【図12】

メッセージ認証子	
追記ブロック#1	追記データ長
	追記データ
追記ブロック#2	
追記ブロック#3	
...	

【図2】



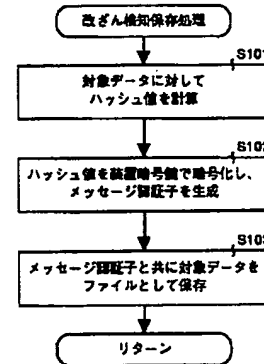
【図4】

鍵データ
鍵の長さ
アルゴリズム

【図5】

年
月
日
時
分
秒
タイムID

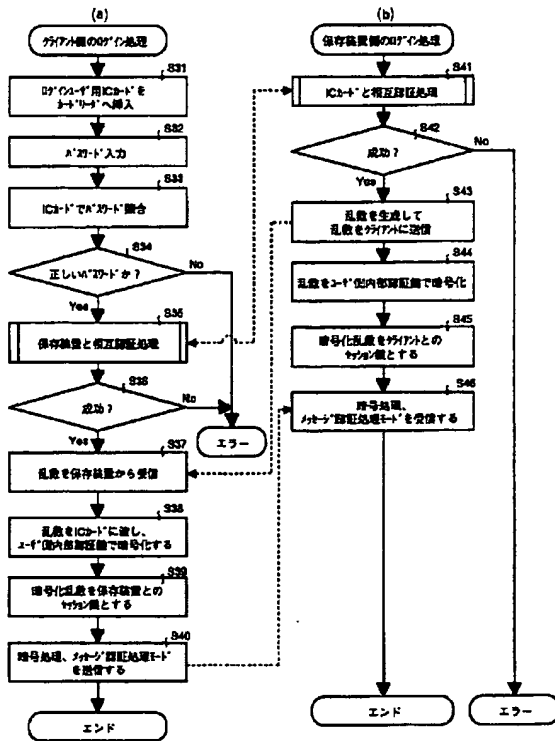
【図10】



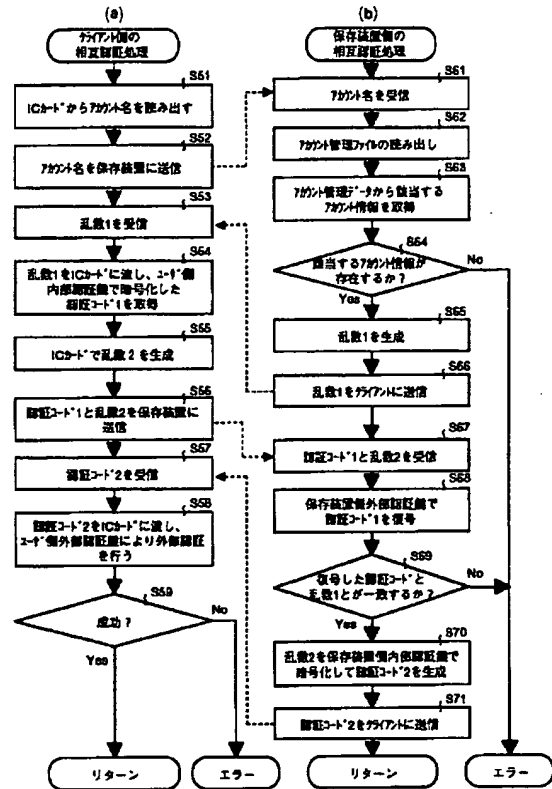
【図15】

タイム設定履歴#1	設定前の日時情報
	設定後の日時情報
	設定したユーザのアカウント名
タイム設定履歴#2	
タイム設定履歴#3	
...	

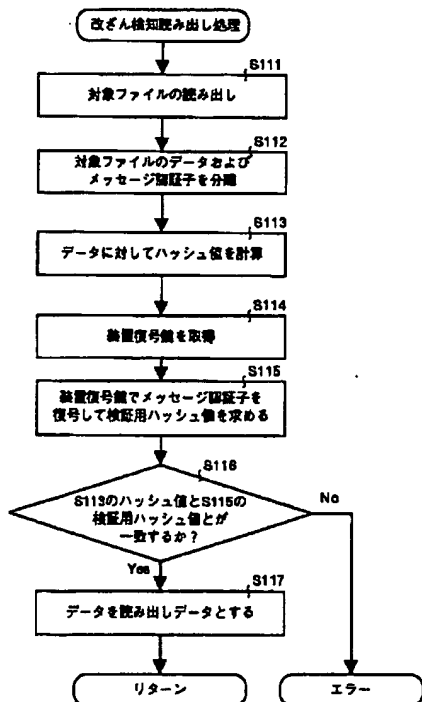
【図6】



【図7】



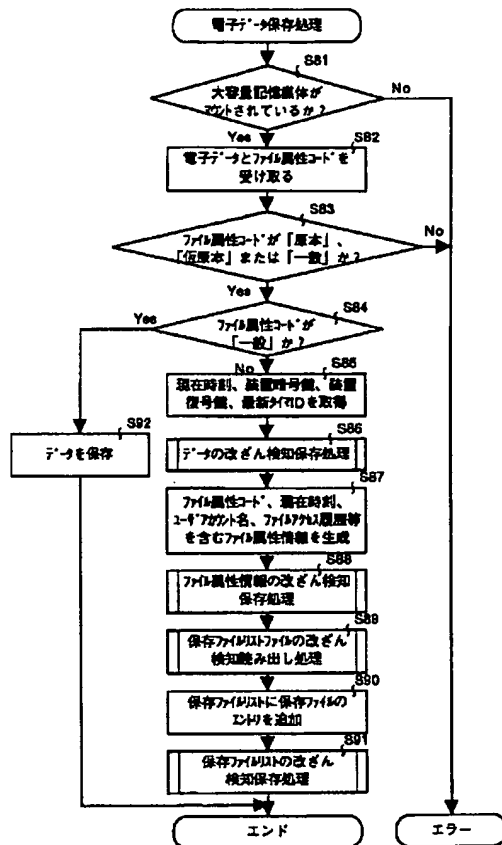
【図11】



【図13】

メッセージ暗号子	
属性管理データ	ファイル名
	ファイルタイプ (ファイルまたはフォルダ)
	ファイルサイズ
	ファイルプロテクトモード (読み出し禁止、書き込み禁止)
	ファイル属性コード (原本、副本、仮原本)
	作成者アカウント名
	ファイル作成日時情報 (タイムID含む)
	更新者アカウント名
アクセス履歴#1	ファイル更新日時情報 (タイムID含む)
	アクセスユーザのアカウント名
	アクセス日時情報 (タイムID含む)
	アクセス識別 (作成、追記、原本化)
保存装置識別番号	
アクセス履歴#2	
アクセス履歴#3	
...	

【図8】



【図14】

メッセージ属性	
リストエントリ#1	有効・無効切り替えフラグ
	ファイル名
	フルパス名
	属性コード
	作成者アカウント名
	更新日時情報
	更新者アカウント名
	原本化実行者アカウント名
	原本化日時情報
	エントリ追加理由 (原本化、原本作成、バックアップ作成、バックアップ復旧)
リストエントリ#2	
リストエントリ#3	
...	

【図16】

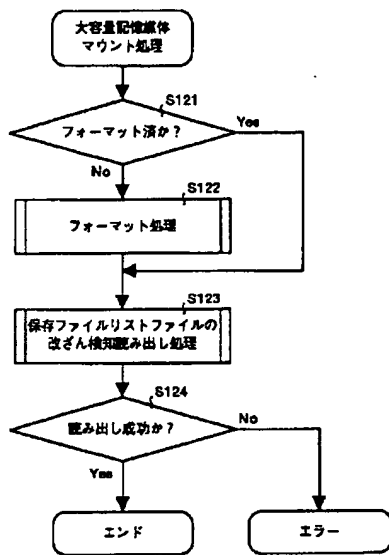
変更前	変更後
19990215 15:32:14 ID=1	19990215 15:30:00 ID=2
19990216 10:21:54 ID=2	19990116 10:22:00 ID=3
19990216 10:45:23 ID=3	19990216 10:46:00 ID=4

【図17】

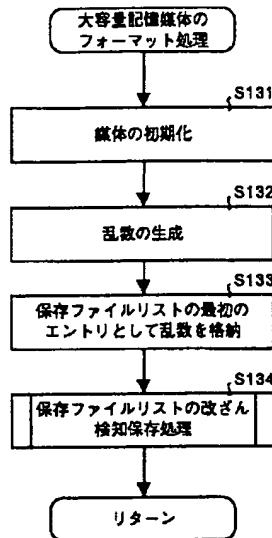
アクセス種別	アクセス日時	装置ID
CREATE	19990215 18:23:10 ID=1	R010-0001032
APPEND	19990215 18:23:30 ID=1	R010-0001032
MOVE TO	19990217 10:10:21 ID=3	R010-0001032
MOVE FROM	19990217 10:13:43 ID=2	R010-0001055



【図18】



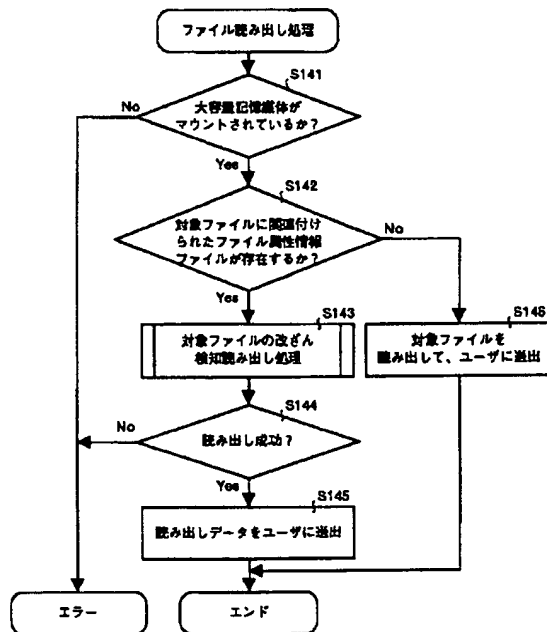
【図19】



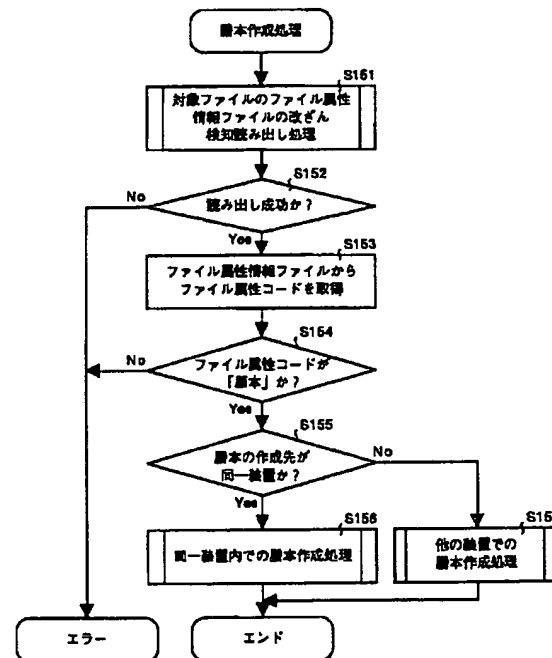
【図33】

復旧前	復旧後
原本	原本
バックアップ仮原本	仮原本
バックアップ原本	原本
バックアップ原本	原本

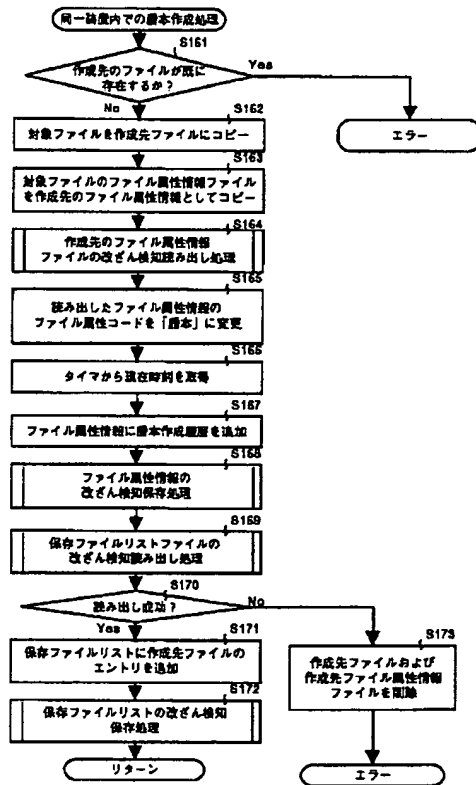
【図20】



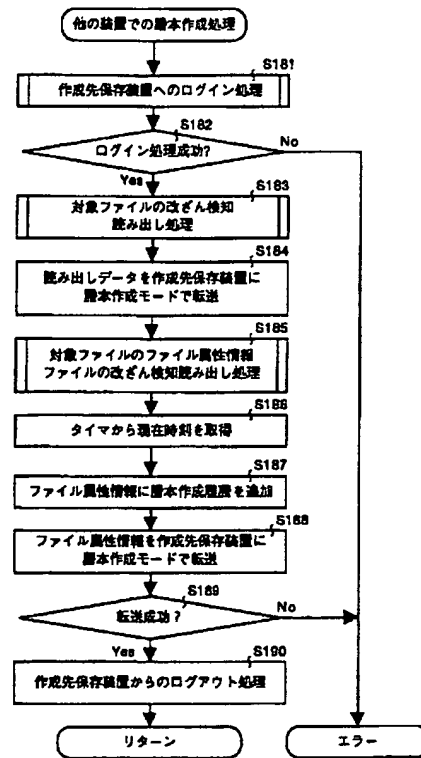
【図21】



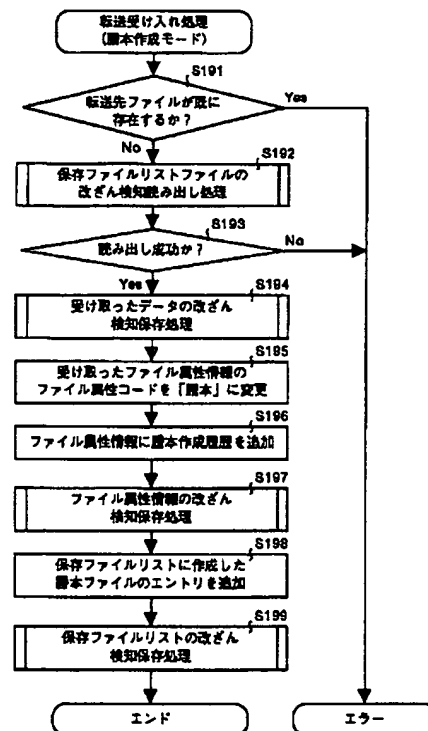
【図22】



【図23】

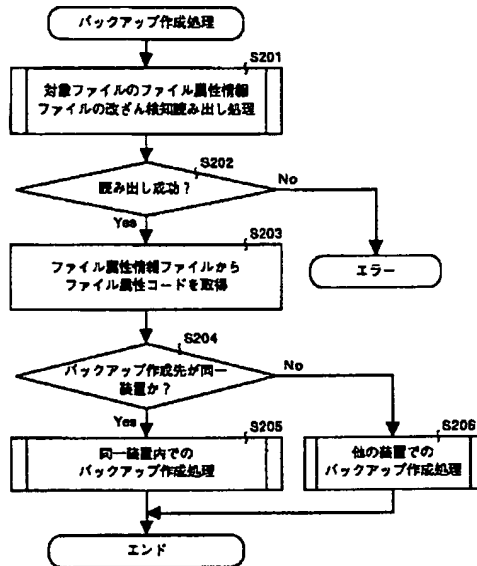


【図24】

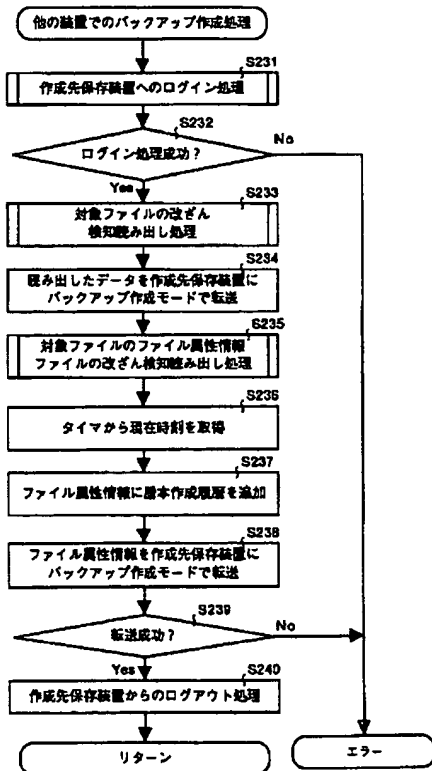




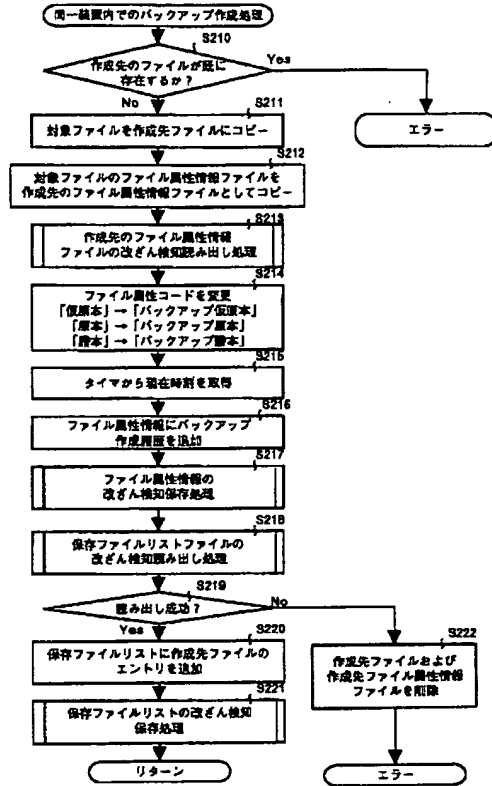
【図25】



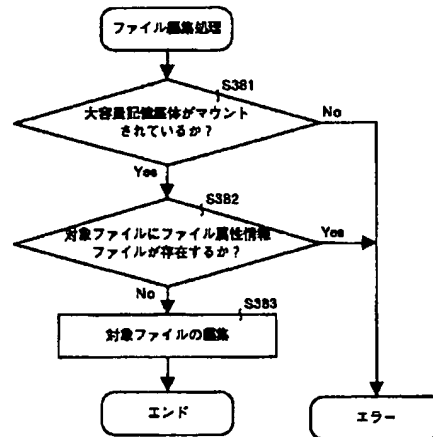
【図27】



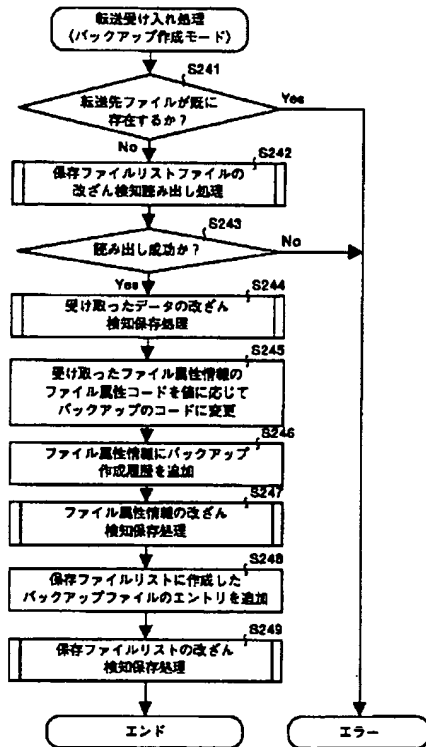
【図26】



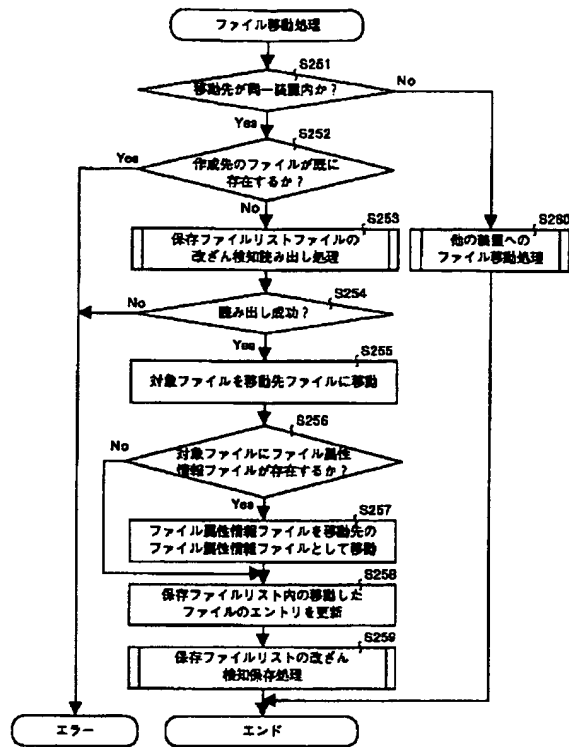
【図37】



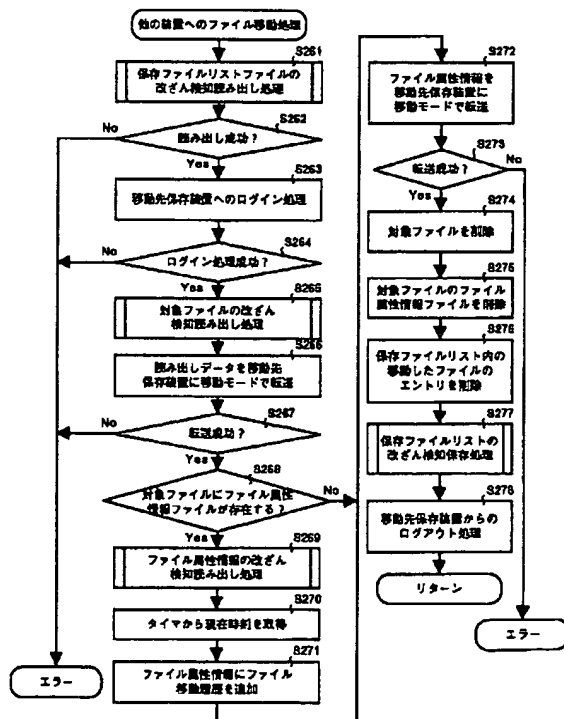
【図28】



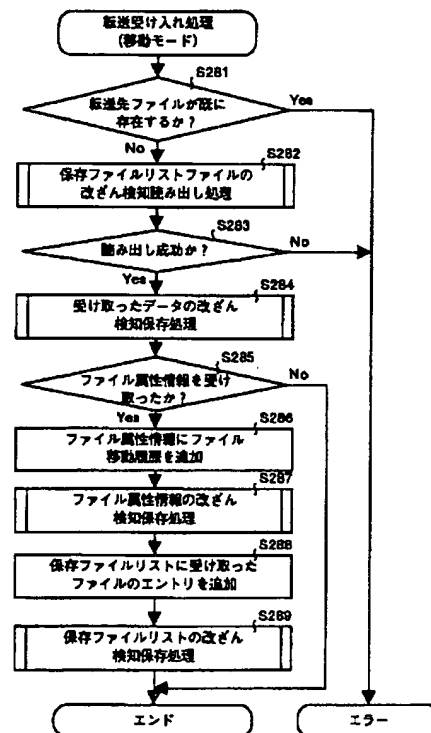
【図29】



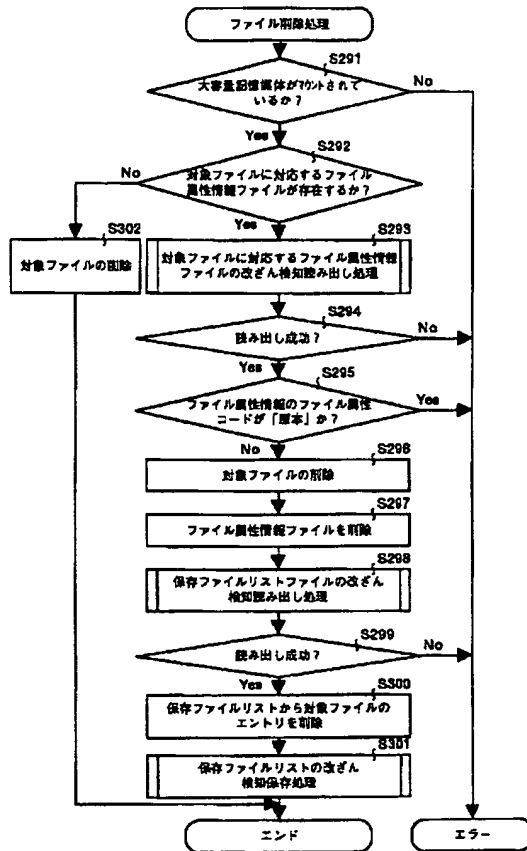
【図30】



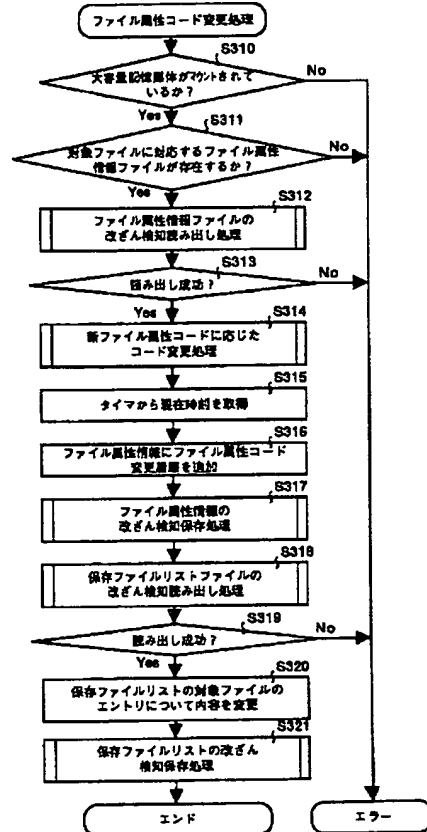
【図31】



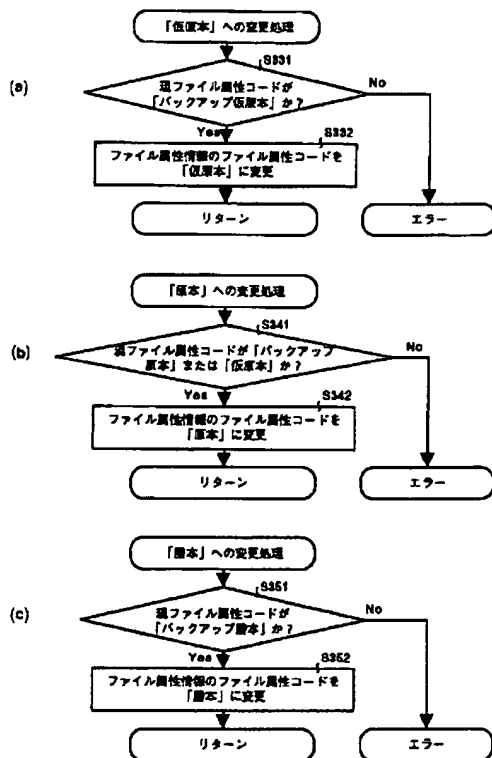
【図32】



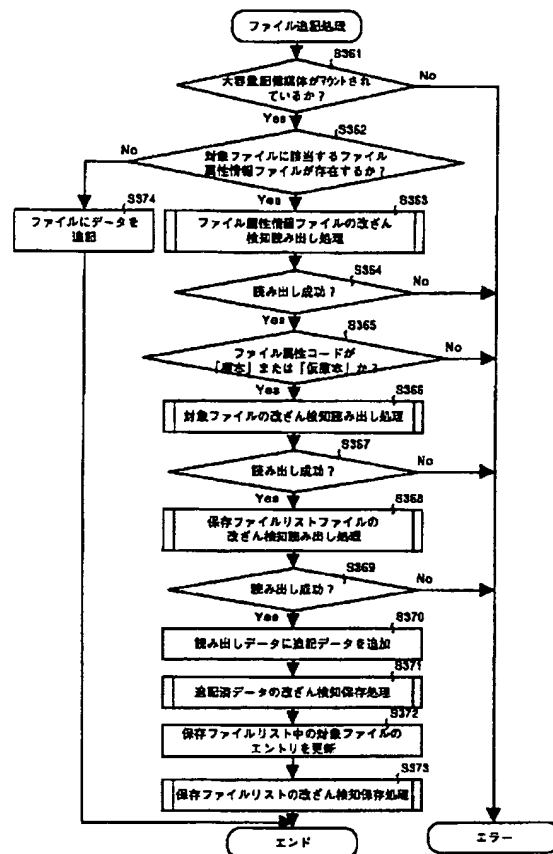
【図34】



【図35】



【図36】



フロントページの続き

- (72)発明者 谷内田 益義  
東京都大田区中馬込1丁目3番6号 株式  
会社リコー内
- (72)発明者 菅生 清  
東京都中央区勝鬃3丁目12番1号
- (72)発明者 戸崎 英一  
東京都中央区勝鬃3丁目12番1号

Fターム(参考) 5B017 AA01 BA05 BA06 BA07 BB10  
CA16  
5B082 AA11 EA10 EA12 GA02 GA13  
GC05 HA08  
5J104 AA08 LA02 NA12 NA35 PA00  
PA14  
9A001 BB04 CZ08 EZ03 HH33 LL03

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☒ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**